SYNŌVIM
HEALTHCARE SOLUTIONS, INC

Best Practices Securing ePHI

Ignite Transformation! Advancing Positive Health Outcomes Through Quality Care

July 31, 2015

Presented by: Trish Harkness, CISSP, CHPS

Acronyms

- BA: Business Associate
- BC/BS: Blue Cross Blue Shield
- BYOD: Bring Your Own Device
- CE: Covered Entity
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- FDA: Food and Drug Administration
- FTC: Federal Trade Commission
- GINA: Genetic Information Non-Discrimination Act
- HIPAA: Health Insurance Portability and Affordability Act
- HIT: Health Information Technology
- IHI: Institute for Healthcare Improvement
- IT: Information Technology
- OCR: Office for Civil Rights
- OIG: Office of the Inspector General
- PCI DSS: Payment Card Industry Data Security Standard
- PHI: Protected Health Information
- SRA: Security Risk Analysis

Objectives

- Recognize the changing health information technology environment
- Understand your risks and how to mitigate them
- Comprehend the regulations and enforcement activities impacting covered entities

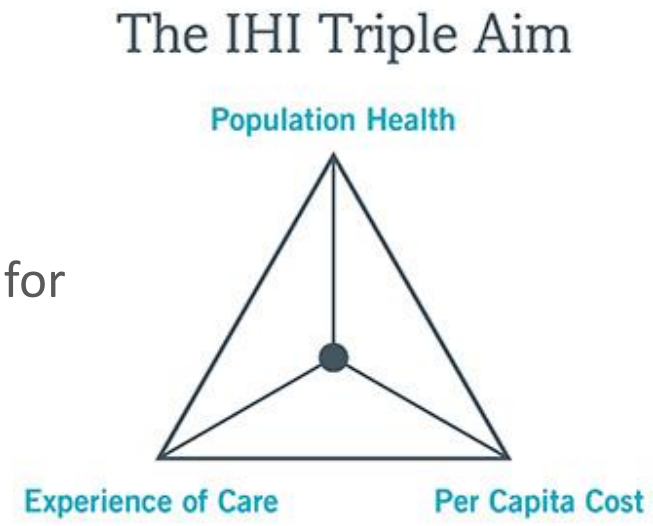
Agenda

- Why Does Information Security Matter?
- Changing Environment of Health IT
- Know Your Risk
- HIPAA Security Rule Compliance
- Beyond HIPAA Compliance

SYNŌVIM HEALTHCARE SOLUTIONS, INC

Why Does Information Security Matter?

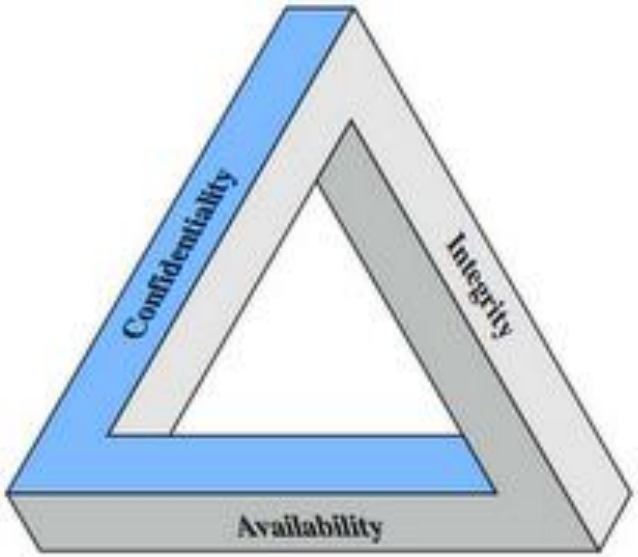
- Healthcare is trending toward advanced payment models
- Triple Aim and EHRs
  - Better care for individuals
    - Clinical decision support
    - Efficient access to health records for healthcare providers as well as patients and their caretakers
  - Better health for populations
    - Accurate population health reports
  - Reducing per-capita costs
    - Reduce duplicative testing and unnecessary services



Graphic from IHI

Health Affairs Blog: *Berwick Brings The 'Triple Aim' To CMS*

Why Does Information Security Matter?



Graphic from
George Moraetes LinkedIn post

- If patients do not trust their healthcare providers to protect their sensitive information:
  - Information provided may be inaccurate or incomplete
  - They may not seek timely care for highly sensitive conditions
- Securing patient data is a critical piece of the health IT puzzle!

Changing Environment of Health IT

- Anthem, Inc. Breach
  - Breach details
    - Anthem-owned unencrypted database was compromised on 12/10/2014
    - Compromise was discovered on 01/27/2015 by a database administrator who noticed his credentials were used to run a query he did not initiate
  - 78.8 million records compromised

CSO Online: *Anthem: 78.8 million affected, FBI close to naming suspect*

Changing Environment of Health IT

- Anthem, Inc. Breach (cont.)
  - Includes customers of
    - Amerigroup
    - Anthem Blue Cross Blue Shield
    - Empire Blue Cross Blue Shield
    - Caremore
    - Unicare
  - May also include customers that used their BC/BS insurance in 14 states served by Anthem
    - California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin

Anthem Facts

Changing Environment of Health IT

- Anthem, Inc. Breach (cont.)
  - Compromised data includes
    - **Names**
    - **Dates of birth**
    - **Social Security numbers**
    - Health care identification numbers
    - Home addresses
    - Email addresses
    - Work information such as income data
  - Compromised data does not appear to include
    - Credit card or banking information
    - Medical information (claims, test results, diagnostic codes, etc.)

Changing Environment of HIT

- Healthcare data is becoming an increasingly valuable target for malicious/criminal hackers
  - It is believed that the value of health data is much more valuable than financial data
    - Medical identity theft is used to receive medical care, buy drugs, submit fake claims, and other activities
    - Financial identity theft is used to open new credit/bank accounts, claim government benefits, get a job, file a false tax return and other activities
  - From 2013 to 2014, the number of people affected by medical identity theft grew 22%
  - Healthcare is “behind the curve” on information security

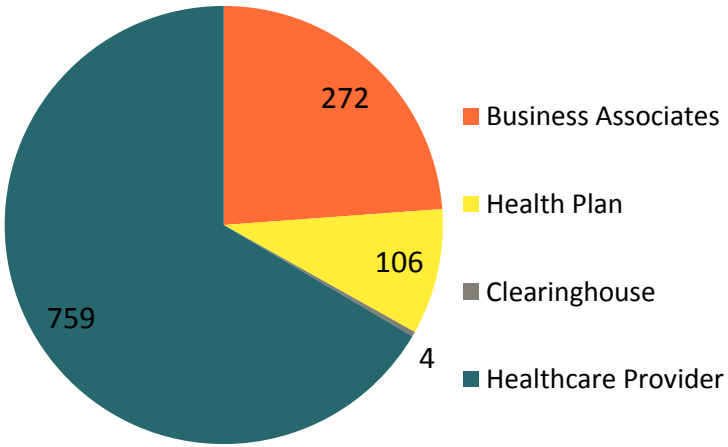
Money and Career CheatSheet: *Why Thieves Want to Steal Your Medical Records*

SYNŌVIM HEALTHCARE SOLUTIONS, INC

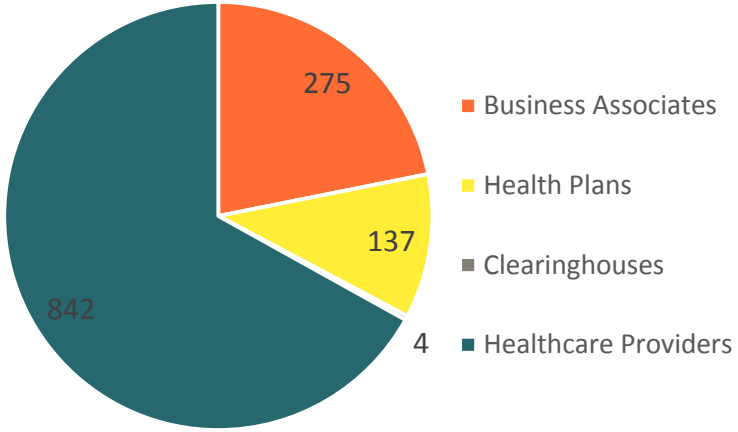
Changing Environment of HIT

Breach Statistics

Number of Breaches by Entity Type as of 02/18/2015



Number of Breaches by Entity Type as of 07/02/2015



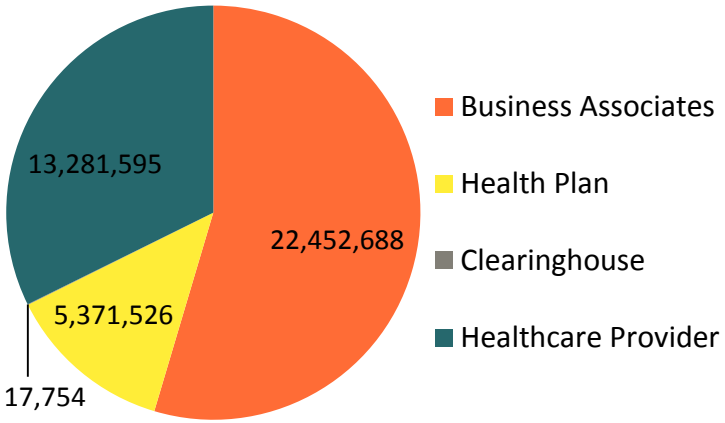
Breach statistics compiled from Office for Civil Rights Breaches Affecting 500 or More Individuals website

SYNŌVIM HEALTHCARE SOLUTIONS, INC

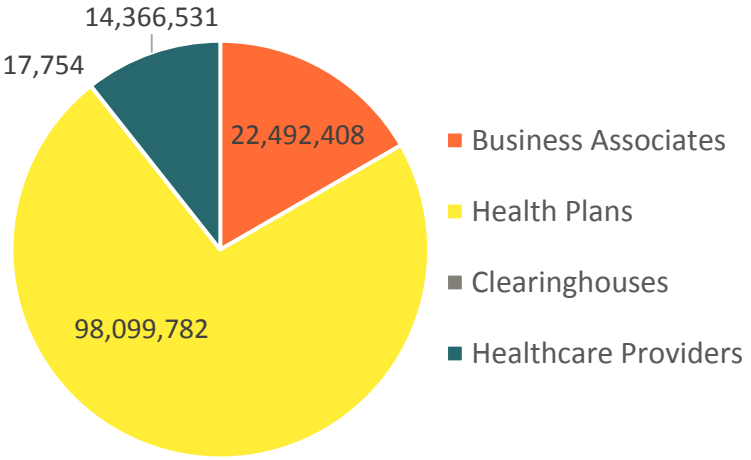
Changing Environment of HIT

Breach Statistics

Lives Affected by Entity Type as of 02/18/2015



Lives Affected by Entity Type as of 07/02/2015

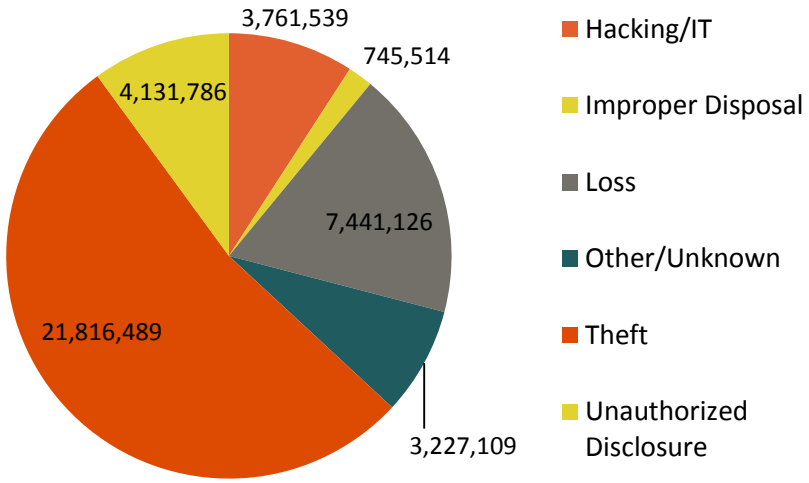


SYNŌVIM HEALTHCARE SOLUTIONS, INC

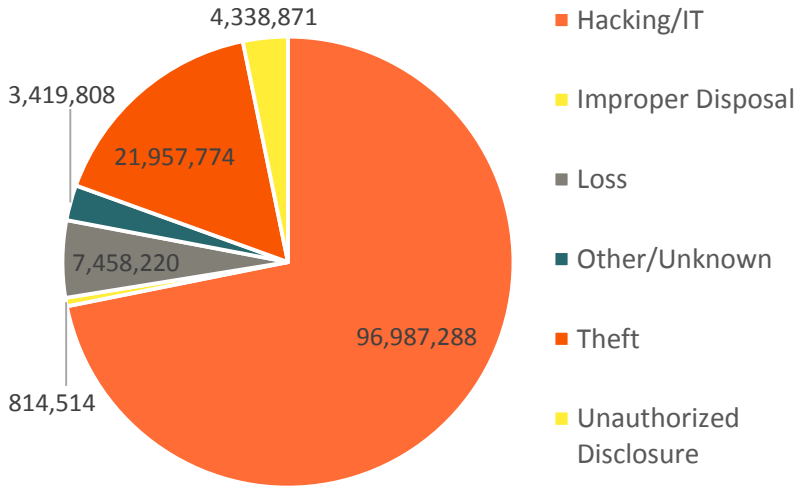
Changing Environment of HIT

Breach Statistics

Lives Affected by Type of Breach as of 02/18/2015



Lives Affected by Type of Breach as of 07/02/015



Know Your Risk

- Is a tornado approaching a school a risk?

CNN Photo

HIPAA Security Rule Compliance

- Security risk analysis and risk management
  - Security risk analysis is not a do-it-and-shelve-it process – it is a ongoing, cyclical improvement process
    - Evaluate your risk
      - Complete your initial SRA to establish a benchmark and start the risk mitigation process
      - Review/update your existing SRA no less than annually
      - As needed, update your existing SRA more frequently for significant planned changes to the information systems
    - Remediate risks in ways that are reasonable and appropriate for your environment
    - Evaluate the effectiveness of remediation activities and (when necessary) alter the remediation activity to improve effectiveness

HIPAA Security Rule Compliance

- Implement control measures
  - Encrypt ePHI at rest and in transit
    - ePHI at rest includes server and hard drive workstations, smart phones, storage devices, removable media, biomedical devices, etc.
    - ePHI in transit is any ePHI that is moving from one recipient to another
  - Assign a Security Official
    - Oversee HIPAA Security compliance program
    - Oversee policy development and implementation
    - Oversee guidance for workstation use
    - Oversee workforce training and education
    - Oversee security incident investigation and breach notification

HIPAA Security Rule Compliance

- Implement control measures (cont.)
  - Implement hiring practices to ensure (as much as possible) that appropriate staff are hired
  - Implement role-based access controls to ePHI
  - Implement physical controls for facilities and sensitive areas within the facility
  - Implement controls to secure workstations
  - Implement controls to secure and track devices and media

HIPAA Security Rule Compliance

- Implement control measures (cont.)
  - Implement routine auditing and evaluations
  - Develop contingency plans
    - Maintain exact copies of ePHI
    - Restore ePHI in the event of loss or corruption
    - Continue providing services during an unexpected event
  - Due diligence and oversight are important with business associates
    - Obtain fully executed BA agreements
    - Determine the most effective method to oversee BA's protection and proper use of your ePHI

HIPAA Security Rule Compliance

- Implement control measures (cont.)
  - Self-insured CEs
    - Must comply with the Genetic Information Non-Discrimination Act (GINA)
  - CEs that also function as a clearinghouse
    - Must separate clinical and practice management functions from the clearinghouse functions

HIPAA Security Rule Compliance

- HIPAA compliance investigations can now be initiated by
  - Patient or workforce member compliant
  - OCR's Permanent Audit Program
  - State Attorneys General
  - Office of the Inspector General during a meaningful use audit

SYNŌVIM
HEALTHCARE SOLUTIONS, INC

Beyond HIPAA Compliance

- Information security is more than just HIPAA compliance
  - HIPAA Security Rule became effective in April 2005 and has undergone minimal change even though the healthcare environment and infrastructure is experiencing significant change
    - Healthcare records are rapidly becoming digital
    - Electronic devices can fit easily in the palm of your hand
    - BYOD is becoming increasingly common for healthcare professionals
    - Use of medical wearables and smart phone health apps is on the rise
    - Removable media can hold a lot of information and is easy to misplace
    - Use of social media is rising

Beyond HIPAA Compliance

- Regulations outside of HIPAA
  - Federal Trade Commission has ruled that HIPAA-covered entities may also be subject to enforcement under the FTC Act
  - Food and Drug Administration is tasked with providing guidance to secure biomedical devices
  - If you store financial information for patients, you need to be PCI DSS compliant

Key Takeaways

- Your first priority should be protecting ePHI with technological and physical controls, not just administrative controls.
- Securing patient data is crucial for timely, accurate patient care as well as healthcare reform initiatives.
- Understanding your risk is critical to protecting PHI and other sensitive data.
- Information security is more than HIPAA Security compliance.
- The balance between protecting information and sharing information is delicate and needs to be evaluated often.

Resources

- Health Affairs Blog: *Berwick Brings The 'Triple Aim' To CMS*
- CSO Online: *Anthem: 78.8 million affected, FBI close to naming suspect*
- Anthem Facts
- Office for Civil Rights Breaches Affecting 500 or More Individuals
- Money and Career CheatSheet: *Why Thieves Want to Steal Your Medical Records*

Guidance

- NIST SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- 800-77: Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs
- Others which are Federal Information Processing Standards (FIPS) 140-2 validated
- NIST SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise

Any Questions?

SYNŌVIM
HEALTHCARE SOLUTIONS, INC

Trisha Harkness, CISSP, CHPS
Senior ISS Services Consultant
Email: trish.harkness@synovim.org

LinkedIn: http://www.linkedin.com/pub/trish-harkness/5/b3/410/

Regional Extension Centers Program
Awardee of The Office of the National Coordinator for Health Information Technology

Synōvim Healthcare Solutions, Inc. is an independent, nonprofit organization sponsored by the Kansas Foundation for Medical Care (KFMC) and the Kansas Association for the Medically Underserved (KAMU). Now the most valued advisor in health information technology throughout the state of Kansas, Synōvim offers proven expertise in EHR implementation & optimization, Meaningful Use assistance and Information Systems Security Management. For more information, visit *synovim.org*.

This material was prepared by the Kansas Foundation for Medical Care, Inc., as part of its work as the Kansas Regional Extension Center, under Grant #90RC0003/01 from the Office of the National Coordinator, Department of Health and Human Services. SYNREC_2015_12