CISSP Seeks CIPP
Object: Mutual Compliance

Marriage of Privacy and Security Professionals Under HIPAA

David B. Nelson, CISSP

Yolo County

Woodland, California

DEMOGRAPHICS

- Yolo County = 180,000 population
- County has 1400 – 1700 workforce members
- One major Mental Health Medicaid program covered by HIPAA (TCS, Privacy, Security, NPI…)
- Contracted out hospital and clinic services for Indigent and Public Health services = BA
- Not a Health Service Agency, but separate departments
- Across the river from State Capitol

Four Points Presentation

1. P&S Married under HIPAA
2. Why Double Certification?
3. Similarities in CISSP and CIPP
4. P&S are MANAGEMENT Activities

P&S Married Under HIPAA

- The RULES
- What we protect and How we protect
- P&S Information Diagram

Married Under HIPAA

- P&S Married at the HIP(AA)
  - "Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. "
  - "Administrative Safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

Married Under HIPAA

- Privacy is WHAT we protect

  WHAT can be driven by law, program or demand.

  HIPAA, SOX, GLB, W&I…

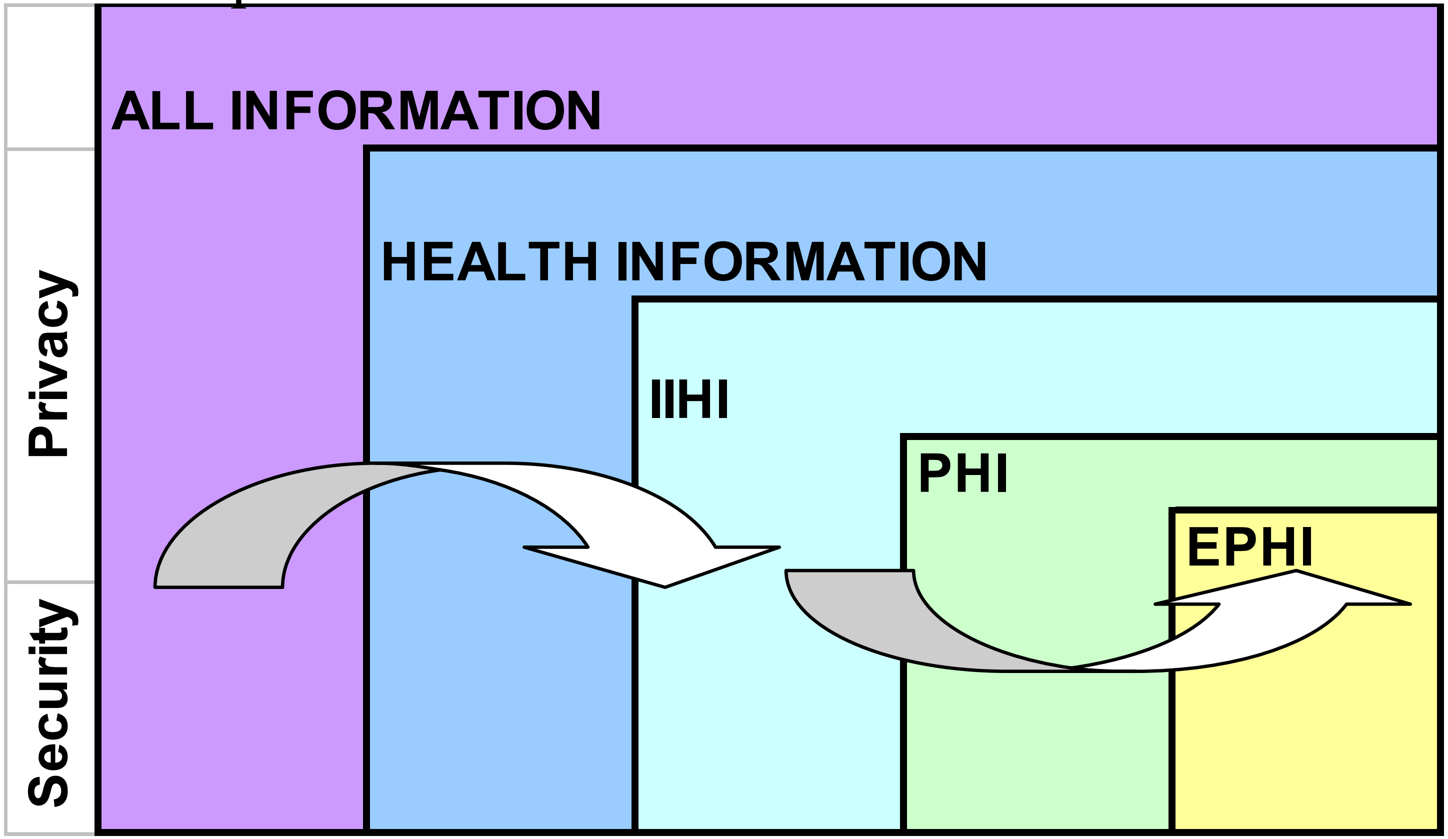
- Security is HOW we protect it

  Physical and technical measures based on data classification

  Locked cabinets, shredders, passwords, IDS, logon review…

Married Under HIPAA

Paper/Verbal------------------------------------Electronic



Privacy

Security

ALL INFORMATION

HEALTH INFORMATION

IIHI

PHI

EPHI

Single Server? Multiple Servers? Internet Servers?

Why Double Certification?

- Benefits
- Two or More
- Just YOU

WHY DOUBLE CERTIFICATION?

- Each has its own benefits
  - One focus is Privacy Rules and Regulations
  - One focus is Security Structure and Management
- How do you PROVE your sincerity? Good Question.
  - For Yolo….
  - Designated Felon Concept (Richard Marks, Esq.)
- Certifications Guarantee Nothing, but…
  - Defined Body of knowledge
  - Guidelines for behavior
  - Outlines International standards
  - On-going education

WHY DOUBLE CERTIFICATION?

Two or More

- 1 CISSP + 1 CIPP = Greater chance of success
- Provides qualified (at least informed) backup
- Best practice to "cross-train"
- Succession Planning for Compliance
  - Compliance Team
  - A "lack" of qualified candidates for these positions
  - Provides a career path for upward mobility

WHY DOUBLE CERTIFICATION?

Just YOU

- Overall entity “expert”
- Single focal point
  - In small entity = I GET EVERYTHING
- Counsel can focus on legal aspect using Expert
- Continuing Education
- Each point has a “bad” reason depending on corporate culture.

Similarities in CISSP and CIPP

- Domains
- Information Security
- Information Infrastructure
- CIPP looks like CISS
- CISSP looks like CIP

Similarities of CISSP/CIPP

CISSP:

Access Control Systems and Methodology
Telecommunications and Network Security
Security Management Practices
Applications and Systems Development
Cryptography
Security Architecture
Operations Security
BCP and DRP
Law and Ethics
Physical Security

CIPP (G):

Privacy Law and Compliance
Information Security
Web Privacy and Security
Data Sharing and Transfer
Workplace Privacy

Additional for Government:
Government Privacy Laws
Government Privacy Practices

CIPP Curriculum Outline

- **Information Security**

A - Definitions - 2 subsets, 6 topics

B - Information Infrastructure - 7 subsets, 22 topics

C - IT Organization - 4 subsets, 28 topics

D - Information Asset Oversight - 3 subsets, 13 topics

E - Information Systems Security - 4 subsets, 28 topics

F - Contingency Planning - 2 subsets, 13 topics

G - Incident Handling - 2 subsets, 15 topics

Information Infrastructure

Information Security

Security Controls

Data Management

Hardware

Internet

IT Management

Networks

Email

Platforms

Reporting Structure

Outsourced activities

Security Roles

Security Awareness Training

Asset Management

Quantifying Assets

Classifying Information Access

Authentication

Authorization

Intrusion prevention

Threats and Vulnerabilities

Disaster Recovery Plan (DRP)

Business Continuance Plan (BCP)

CIPP Looks Like CISSP

- **Hardware**

Client systems, Handheld, Servers, Storage, Desktop, Laptop

- **Platforms**

Mainframes, Desktops, Wireless/Portable Devices

- **Networks**

Local Area Networks/Wide Area Networks (LAN/WAN), Mobile and Wireless, Telecom, Ethernet and Optical, Broadband – Digital Subscriber Line (DSL), Voice Over IP Protocol (VoIP)

- **Internet**

Web, E-Commerce, E-Business

- **Data Management**

Backups, Database management, Recovery

CISSP Looks Like CIPP

Titles from study guide

- **Law Investigations and Ethics**

Cyber law, Computer Ethics Institute, Internet Architecture Board, Generally Accepted System Security Principles (GASSP), Motive opportunity and means

- **Hackers and Crackers**
- **Well Known Computer Crimes**
- **Liability and its Ramifications**
- **Types of Law**
- **Discarding Equipment and Software Issues**
- **Computer Crime Investigations**
- **Import Export Laws**
- **Privacy** (2 pages in Shon Harris' "All-In-One CISSP Certification") SOX, GLB

MANAGEMENT

- Policy Procedures vs. Security
- Yolo Management Outline

It is “Management”

- Management is the KEY word

  Generally Speaking
  - CIPP for Privacy is most of Policy and Procedures
    - Version Control, Review Period, Training
  - CISSP for Security is the electronic half of information
    - Understand/Know where vulnerabilities are
    - Choose solutions that minimize RISK to an acceptable level

Yolo Management Outline

- **Defining Security Principles**
- **Security Management Planning**
- **Risk Management and Analysis**
- **Policies, Standards, Guidelines, and Procedures**
- **Examining Roles and Responsibility**
- **Management Responsibility**
- **Understanding Protection Mechanisms**
- **Classifying Data**
- **Employment Policies and Practices**
- **Managing Change Control**
- **Security Awareness Training**

SUMMARY

By yourself or as a team the awareness of the combined impacts of privacy and security compliance it is best served by having both CISSP and CIPP certification.