The Interdependency of Privacy, Technology & Compliance

The First National HIPAA Summit

Healthcare Strategy Institute

October 17, 2000 11:00 - 12:00 am

Grand Hyatt, Washington, DC

Margret Amatayakul

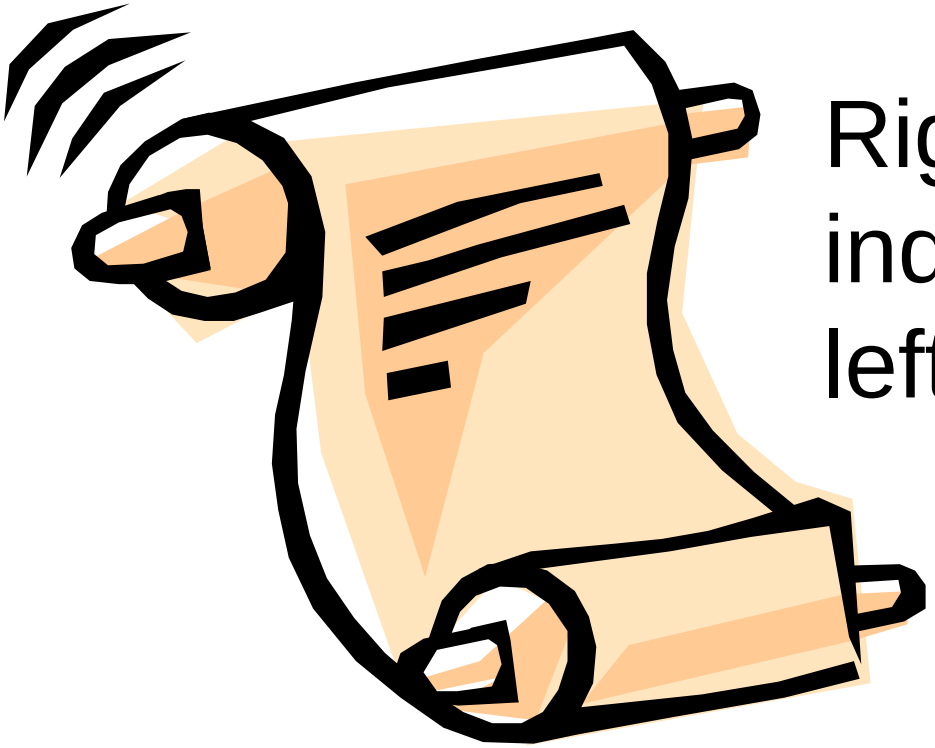
Margret\A Consulting, LLC

Agenda

- What is privacy?
- What is security?
- How are privacy and security related?
- How are they different?
- What is compliance?
- How do you become compliant?

What is Privacy?

Privacy



Right of an individual to be left alone

Privacy Directives

- Professional codes of conduct
  - Hippocratic Oath
  - AHA Patient's Bill of Rights
- Accrediting and licensing standards
  - JCAHO/NCQA
  - Conditions of Participation
  - State licensure
- Business practices
  - Proprietary interests
  - Business records rules
- Consumer influence

Privacy Law

- Freedom of Information Act of 1966
  - Applies to records pertaining to the executive branch of the federal government
- Privacy Act of 1974
  - Applies to healthcare organizations operated by the federal government
- 42 C.F.R. Part 2
  - Applies to federally-assisted facilities that provide a substance abuse program
- Uniform Health-Care Information Act
  - *drafted* by National Conference of Commissioners on Uniform State Laws, February 11, 1986
- Bills, bills, bills

. . . is elusive!

Tracking Federal Medical Privacy Legislation

- Text of bills
  - http://thomas.loc.gov
- Progress
  - American Health Information Management Associations
  - www.ahima.org
- Issues
  - Electronic Privacy Information Center
  - www.epic.org

HHS Secretary Shalala Privacy Principles

- **Boundaries:** Individual information should be used for health purposes only, subject to few exceptions. It should be easy to use information for defined purposes; very difficult to use for other purposes
- **Security:** Federal law should require those to whom we entrust health information to protect it against deliberate or inadvertent misuse or disclosure
- **Consumer Control:** Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them
- **Accountability:** Those who misuse information should be punished, and those who are harmed by its misuse should have legal recourse
- **Public Responsibility:** Privacy must be balanced by public responsibility to contribute to the common good. This include oversight, public health, research, and law enforcement

What is Security?

Security

Technology
that guards:

- confidentiality
- data integrity
- availability

Confidentiality

- The act of limiting disclosure of private matters
- Security measures that contribute to confidentiality include those which:
  - Limit access
    - Access control
    - Encryption
    - Entity authentication
  - Monitor access
    - Accountability
    - Auditing
    - Chain of trust

Consequences

- To the individual
  - Loss of personal dignity
  - Discrimination in hiring, housing, loan applications, and other social interactions
- To the provider
  - Image damaged
  - Potential lawsuit
  - HIPAA civil and criminal penalties
  - Impact on accreditation, licensure, participation
- To the industry
  - Loss of credibility
- To the nation
  - Change in the course of history

Data Integrity

- The property that data have not been altered or destroyed in an unauthorized manner
- Security measures that contribute to data integrity include:
  - Access controls
  - Data authentication
    - Check sum
    - Parity checks
    - Digital signature
  - Key management
  - Message authentication checks
  - Virus checking

Consequences

- Quality of care
  - Repeat procedures
  - Misdiagnosis
  - Treatment errors
- Harm to patient
  - Inconvenience
  - Illness/injury exacerbated
  - Iatrogenic condition
- Cost of care
  - Extended length of stay
  - Additional services
  - Liability
  - Malpractice insurance

Availability

- The property of being accessible and useable upon demand by an authorized entity
- Security measures that contribute to availability include:
  - Security configuration management
    - Installation
    - Maintenance
    - Backup
  - Contingency planning and disaster recovery
  - Appropriately chosen technical security services

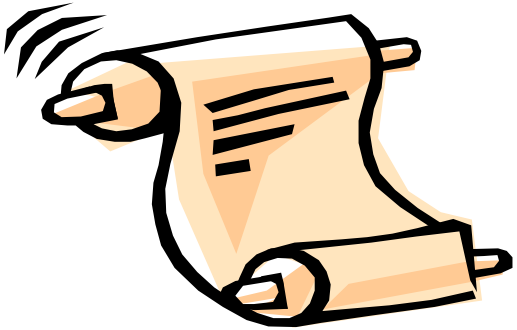
Consequences

- Patient care
  - Loss of critical time in emergency
  - Delayed care
  - Errors
- Practitioner productivity
  - Annoyance
  - Loss of productivity
  - Distrust in system

How are Privacy & Security Related?

Co-dependent

Privacy principles drive security

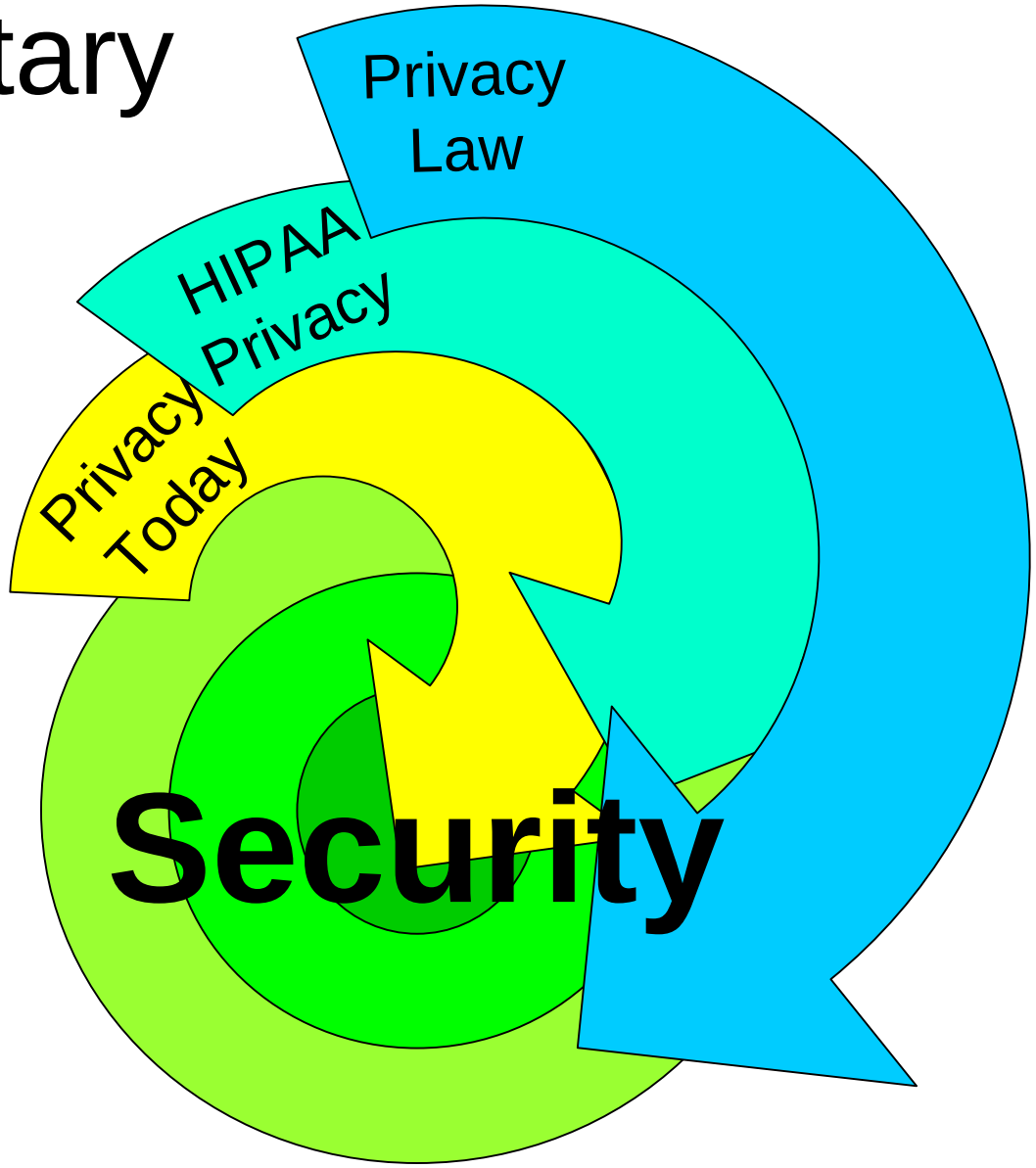


Security protects privacy

Policy Required by Security

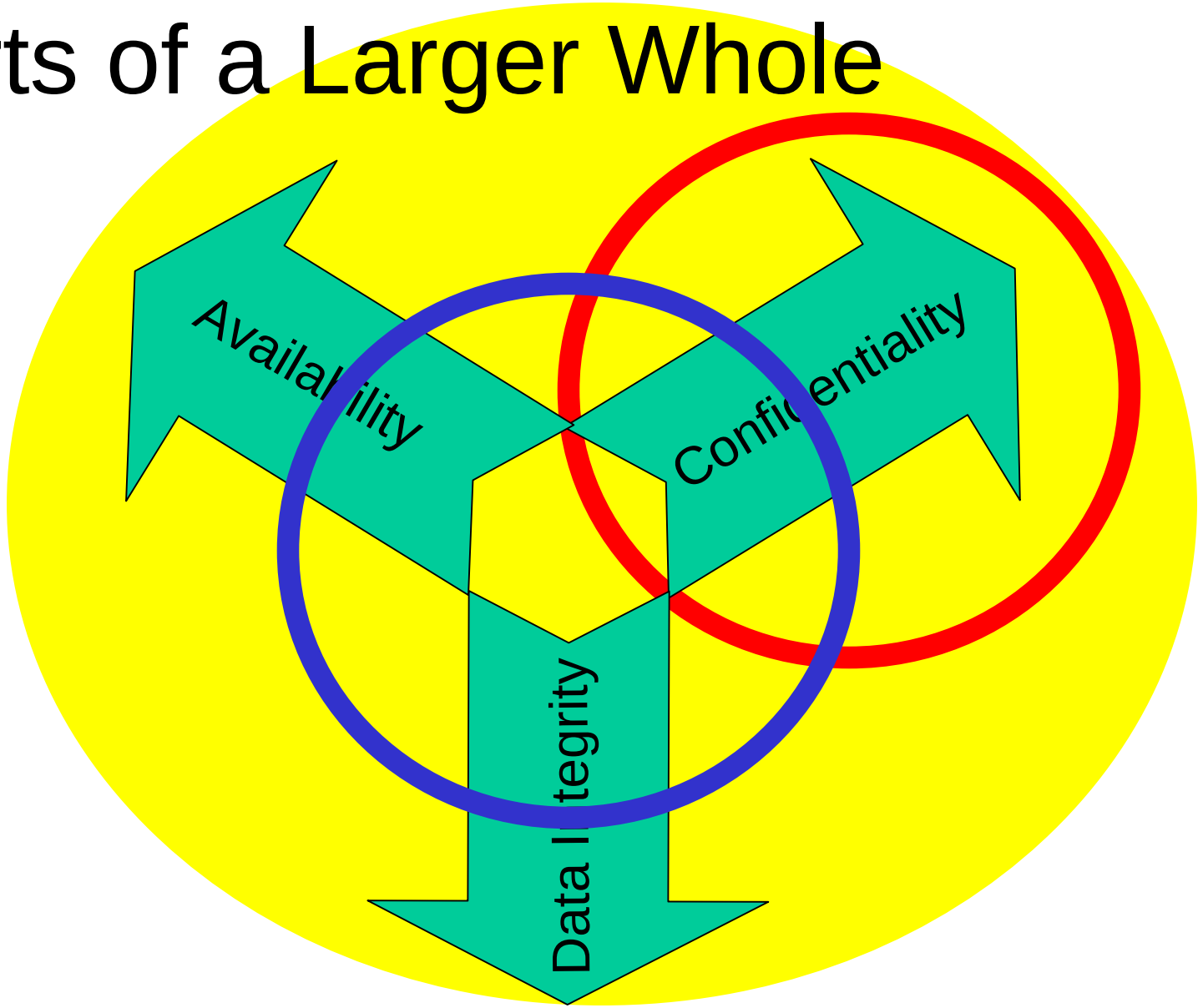
- Access control
  - What form/what rules
    - User-based
    - Role-based
    - Context based
- Audit control
  - What form
  - How frequently
  - What level
- Entity authentication
  - What form of unique user identification
    - User identification
    - Passwork
    - PIN
    - Biometric
    - Token

Complimentary



How are Privacy & Security Different?

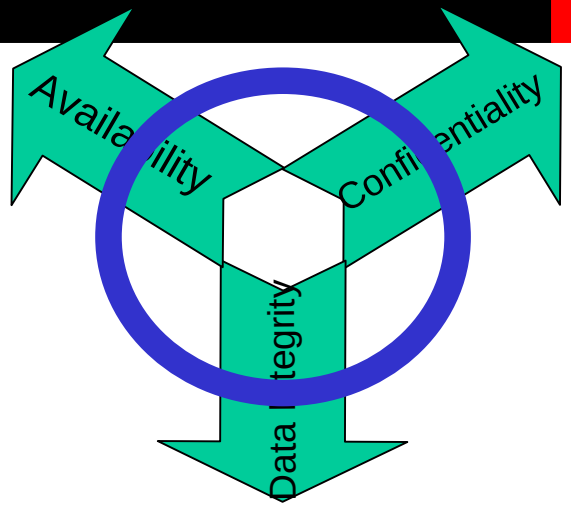
Parts of a Larger Whole



Contradictory

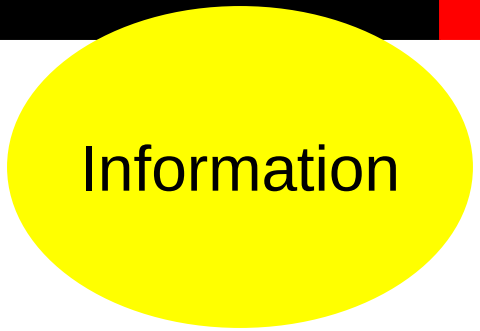
- Confidentiality
  - Is required when one person has shared private information with another person
  - Requires protection of information
- Availability
  - May be opposite of confidentiality
  - Requires accessibility to information
- Fear of breach of confidentiality may result in private information not being available for care

Security Measures



- Security affords
  - protection for confidential information
  - assurance that information will be available
  - reduces potential for alteration or destruction of information
- Security only operates on the information system (although the system should not be limited to electronic)
- Security may provide reminders and training for people, but cannot alter human practice

Health Information



- Health information
  - Health status
  - Health care services
  - Payment for health care services
  - Operational provision of health care services
- Health “care” information implies limited scope
- Individually identifiable health information
  - Is a subset of health information, including that which identifies an individual
- Protected health information
  - Under HIPAA, individually identifiable health information that is or has been electronically maintained or transmitted

What is Compliance?

Compliance

- Definition
  - the act of conforming, cooperating; being obedient
- Subject
  - the entity conforming; in HIPAA, “covered entities” include providers, payers, and clearinghouses
- Object
  - that on which the subject must conform; in HIPAA, these are standards

Standards

- Definition
  - Authority by general consent
  - Most common size or form
  - Rule or principle that is the basis of judgment
  - Average or normal quality, quantity, ethics, customs, etc. regarded generally as acceptable
  - Authorized exemplar
- In HIPAA
  - Standards may be specific requirements
    - Established by government
    - Adopted from industry
  - Standards are also frameworks (i.e., skeletal structure of something)

HIPAA Standards

- Specific
  - ASC X12N for financial and administrative transactions
  - ICD-9-CM, CPT-4, CDT-2, NDC for code sets
  - National Provider Identifier
  - FEIN for employer identifier
- Framework
  - Electronic transactions options for providers
    - Paper
    - Technology
  - Security standards based on risk analysis
  - Notice of information practices based on entities' practices
  - Amendment at provider's discretion

Benefits and Risks

- Benefits
  - Technology neutral
  - Scalable
  - Accommodates risk profile of covered entity
- Risks
  - Variation will not achieve a common standard
  - Interpretation problems
  - Industry has not previously adopted standards, so unlikely to be willing to benchmark

Becoming Compliant

Who is to be Compliant

- Covered entities
  - Providers
  - Clearinghouses
  - Health plans

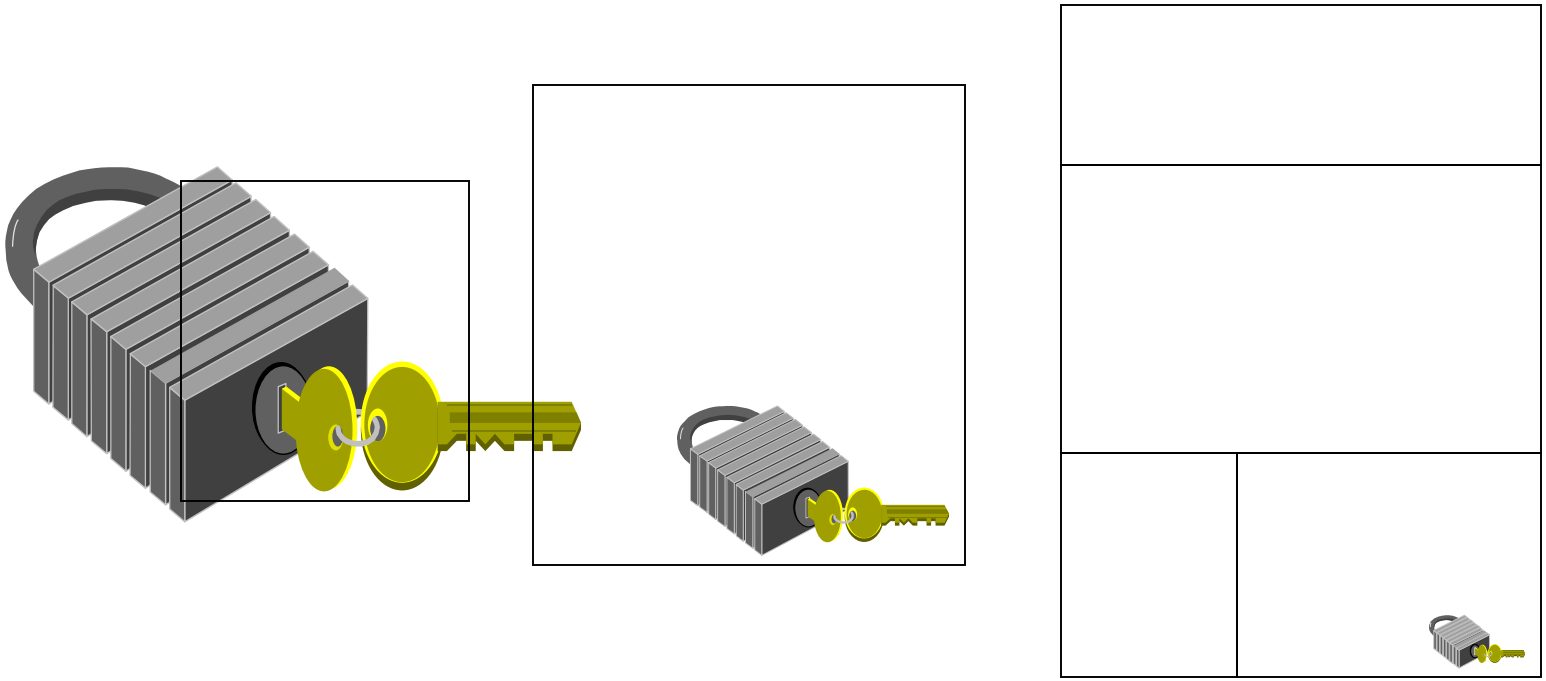
- Vendors
- Suppliers
- Employers
- Others

- Vendors should supply products and services that enable compliance
- Suppliers must accept business associate agreement
- Employers are often providers and/or health plans in part

Risk Assessment

- HIPAA requires
  - "each affected entity to assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements"
  - "How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make"
- Vendors can and should supply products and services that meet *your* needs,
- but their products and services *alone* do not make you compliant

One Size Does Not Fit All



Contact:

Margret Amatayakul

Margret\A Consulting, LLC

1817 Georgia Ct. #202 ■ Schaumburg, IL 60193

Tel. 847-895-3386 ■ Fax. 603-853-6571

E-Mail. MargretCPR@aol.com ■ www.Margret-A.com