HIPAA Privacy Regulations: Policy and Technology Implications

Margret Amatayakul, RHIA, FHIMSS

President

Margret\A Consulting, LLC

Schaumburg, IL

Agenda

- **What is privacy?**
- **What is security?**
- **How are privacy and security related? How are they different?**
- **What privacy policies are required for HIPAA?**
- **What technology is needed to support HIPAA privacy?**

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, CARF, etc.
  - Conditions of Participation
  - State licensure and other laws

- **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, 1986

- **Bills, bills, bills**   . . . is elusive!

HHS Secretary Shalala Privacy Principles

- **Boundaries:** Easy to use for health care, difficult for to use for any other purpose

- **Security:** Federal law should afford protection

- **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:** Misuse should be punished, and those harmed should have legal recourse

- **Public Responsibility:** Privacy must be balanced by public responsibility to contribute to the common good

What is Security?

Security

Safeguards:
C - onfidentiality
I - ntegrity
A - vailability

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

Before

After

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

Integrity

- **Property that data have not been altered/destroyed in unauthorized way**
- **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**

12

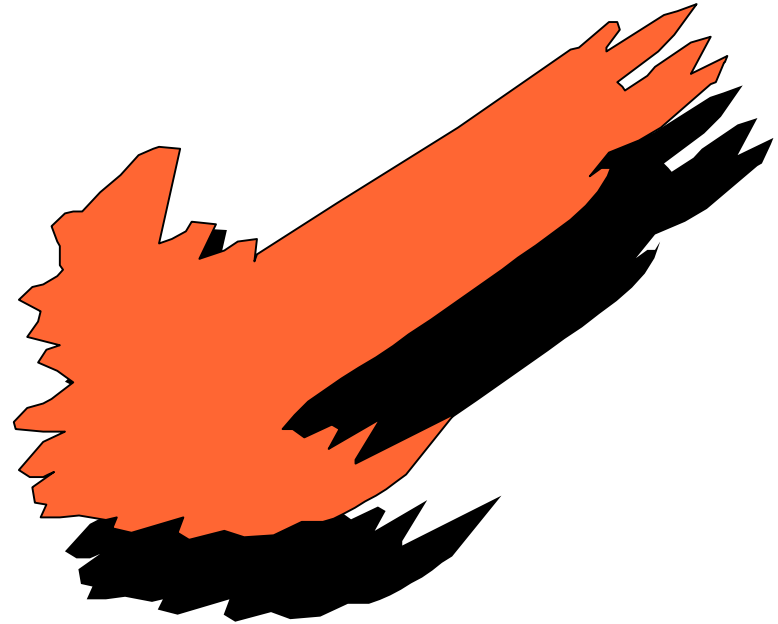# Consequences

- ## 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

- **Property of being accessible/useable upon demand by authorized entity**
- **Security measures that contribute to availability include:**
  - Security configuration management
    - ◆ **Installation**
    - ◆ **Maintenance**
    - ◆ **Backup**
  - Contingency planning
  - Disaster recovery
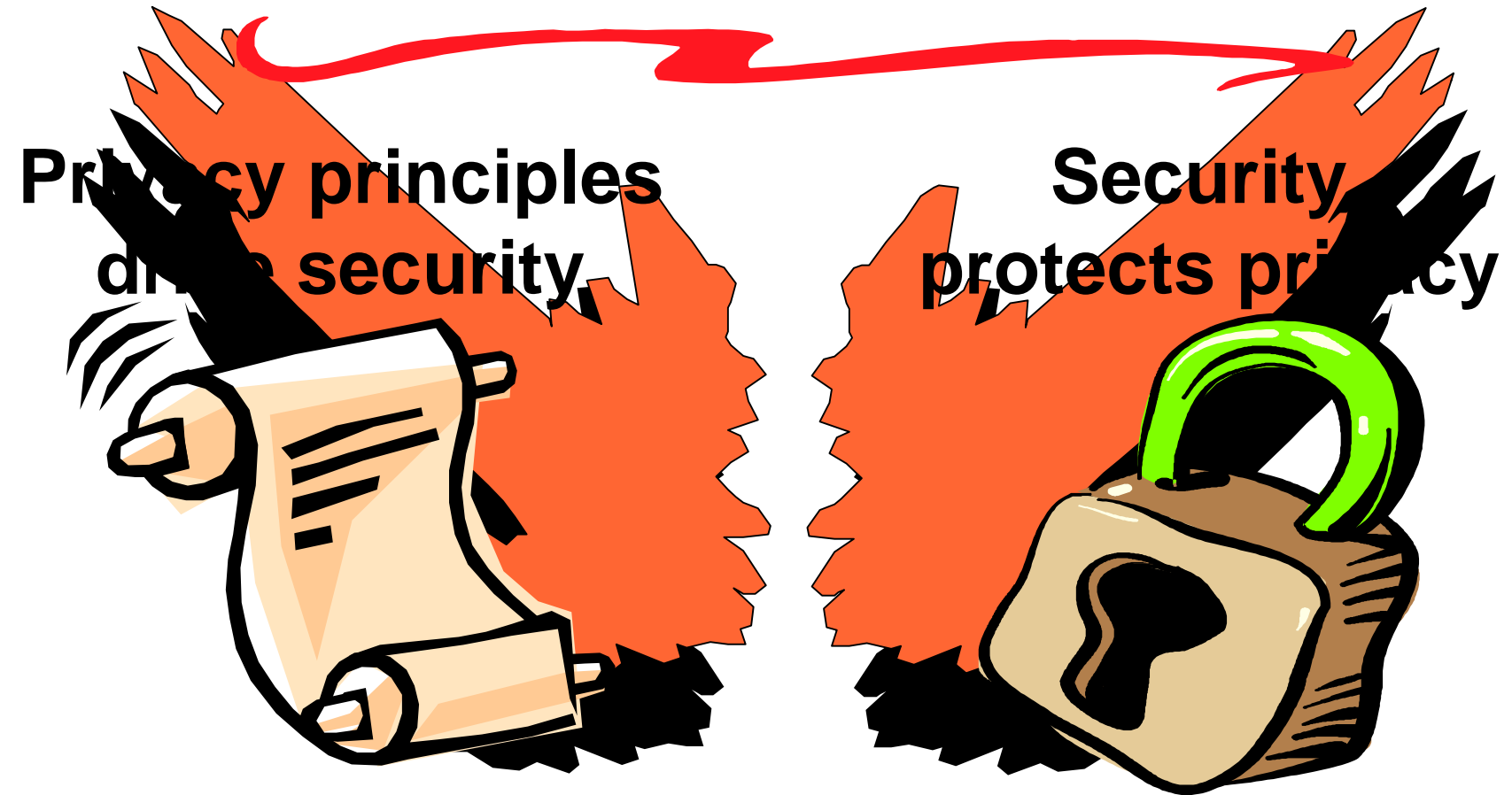 - Appropriately chosen technical security services

Consequences

- **Patient care**
  - Loss of critical time in emergency
  - Delayed care

  - Errors

- **Practitioner productivity**
  - Annoyance
  - Loss of productivity
  - Distrust in system

How are Privacy and Security Related?

Co-dependent

Privacy principles drive security

Security protects privacy

Contradictory

- **Confidentiality**
  - Is required when person has shared private information with another
  - Requires protection of information

- **Availability**
  - be opposite of confidentiality
  - Requires accessibility to information
  - Fear of breach of confidentiality may result in private information not being av

Privacy Standards

Privacy Standards

- ## Uses and disclosures
    - Permitted, and required (only to individual and Secretary of HHS)
    - Minimum necessary, except for treatment
    - Subject to agreed upon restriction
    - De-identified protected information
    - Disclosures to business associates require assurance of safeguards through contract
    - Deceased individuals same protection
    - Personal representative treated as individual
    - Alternative means or locations to receive confidential communications
    - Uses and disclosures consistent with notice
    - Whistleblower protections

Standards, Con't.

- **Consent** for uses and disclosures to carry out treatment, payment, or operations
  - Consent requirements
  - Conflicting consents
  - Joint consent
- Uses and disclosures for which **authorization** is required
- Uses and disclosures requiring **opportunity** for individual to agree or object
  - Facility directories
  - Involvement in care
- Uses and disclosures for which consent, authorization, or opportunity to agree or object is **not required**

Standards, Con't.

- ## Organizational requirements
  - Healthcare component of hybrid entity
  - Affiliated covered entities
  - Business associate contract
  - Requirements for group health plans
  - Multiple covered functions

- ## Other requirements
  - How to de-identify information
  - Minimum necessary use, disclosure, and request
  - Marketing
  - Fundraising
  - Underwriting
  - Verification requirements

Standards, Con't.

- **Right** to notice of privacy practices
- **Right** to request privacy protections
  - Right to request restrictions on uses or disclosures
  - Right to request confidential communications
- **Right** of access to inspect and copy information
  - Unreviewable grounds for denial
  - Reviewable grounds for denial and review process
- **Right** to amend information
  - Accepting and notifying others
  - Denial, disagreement, rebuttal, and documentation
  - Future disclosures must include documentation or summary
- **Right** to accounting of disclosures except to carry out treatment, payment, operations

Privacy, Con't.

- ## Administrative requirements
  - Privacy officer
  - Training
  - Safeguards
  - Complaints
  - Sanctions
  - Duty to mitigate harmful effects
  - Refrain from retaliation
  - May not waive rights
  - Policies and procedures/changes
  - Documentation

- ## Transition provisions

What Policies?

Policy Characteristics

- **Reflect the culture of the organization**
- **Represent stable, long-term plans within which objectives may be set and decisions made**
- **Effective policies require judgment but not complex interpretation**
- **Must be consistent throughout the enterprise**
- **Developed by senior management &/or expert committee; approved by senior management and board of directors**

Policies vs. Procedures

- ## Policies
  - Establish goals that technical mechanisms serve
  - Outline appropriate uses and disclosures of information
  - Create mechanisms for preventing and detecting violations
  - Set rules for disciplining offenders

- ## Procedures
  - Describe how to carry out policies
  - Provide forms and formats for processing policies

- ## Both must be documented, and training, education, and awareness applied to effect culture change

Policy Development

- **Inventory policies that exist already**
  - Medical Staff Bylaws, Rules, and Regulations
  - Management - consolidated or in departments
  - Human Resources
  - Public Relations

- **Determine practice variances:**
  - Medical Record Department
  - Information Systems
  - Admissions/Registration
  - Patient care
  - Administration
  - Physician practices

- **Compare with HIPAA standards**
- **Relate to technology needs**

Policy Inventory

Requirement	Policy	Date	Variance	Rev?	Technology
Termination Procedures	HR 236	R96	Med Staff	Y	ACL Renewal Audit Trail
Awareness Training	None		Med Recs	Y	Tracking
De-identify	MR 101	R95	E.D.	Y	Mask fields

What Should Be Included

- **Subject**
- **Statement of purpose**
- **Policy statement**
- **Definitions**
- **Responsibility for associate procedures and implementation**
- **Authority**
- **Effective Date**
- **Rider that authenticates receipt, understanding, agreement to abide by**

Policy Example

St. Margret's Hospital

PURPOSE:
To best serve our patients and provide our medical staff and employees with the best possible resources, St. Margret's Hospital adopts and makes use of new means of communication and information exchange. This means that many staff and employees have access to one or more forms of electronic media and services, including fax fax machines, voice mail, e-mail, and services provided through the Internet.

POLICY:
St. Margret's Hospital encourages the use of electronic media and associated services because they can make communications more efficient and effective and they are valuable sources of information. However, all members of the medical staff, employees, and others affiliated in any manner with the Hospital should remember that electronic media and services provided by the Hospital are property of St. Margret's Hospital and their purpose is to facilitate and support the Hospital's business. This policy will provide the philosophy and guidelines for utilizing these electronic media and services.

This policy applies to all electronic media and services that are: accessed on or from St. Margret's Hospital,accessed using St. Margret's Hospital computer equipment or via St. Margret's Hospital paid access methods, or used in a manner that identifies the ind with St. Margret's Hospital.

31

Page 2

1. Prohibited communications

Electronic medial and services cannot be used for knowingly transmitting, retrieving, or storing communication that is:

    a. Discriminating or harassing

    b. Derogatory to any individual or group

    c. Obscene, sexually explicit, or of a pornographic nature

    d. Defamatory or threatening

    e. Engaged in for any purpose that is illegal or contrary to St. Margret's Hospital policies or business interests

2. Personal use

Electronic media and services are provided by St. Margret's Hospital solely for the purpose of carrying out St. Margret's Hospital business. Therefore, everyone with access to such media and services are expected to demonstrate a sense of responsibility and not abuse this privilege.

3. Access to communications

Electronic information created and/or communicated by a member of the medical staff or an employee using any electronic media may be monitored by St. Margret's Hospital. Individual use patterns, such as Internet sites accessed, e-mail sent, telephone numbers dialed, call length and time at which calls are may may be monitored for cost analysis, resource ut and detecting patterns of use that indicate violation of Hospital policies.

Policies & Outside Attacks

- **Policies are most effective in protecting against abuses by legitimate system users:**
  - HIPAA "workforce:"
    - Employees
    - Medical staff
    - Students/faculty
    - Volunteers
  - Contractors/vendors/temporary employees/payers/other third parties (via business associate agreement)

- **Policies can provide guidance for establishing mechanisms to protect against outside attackers**
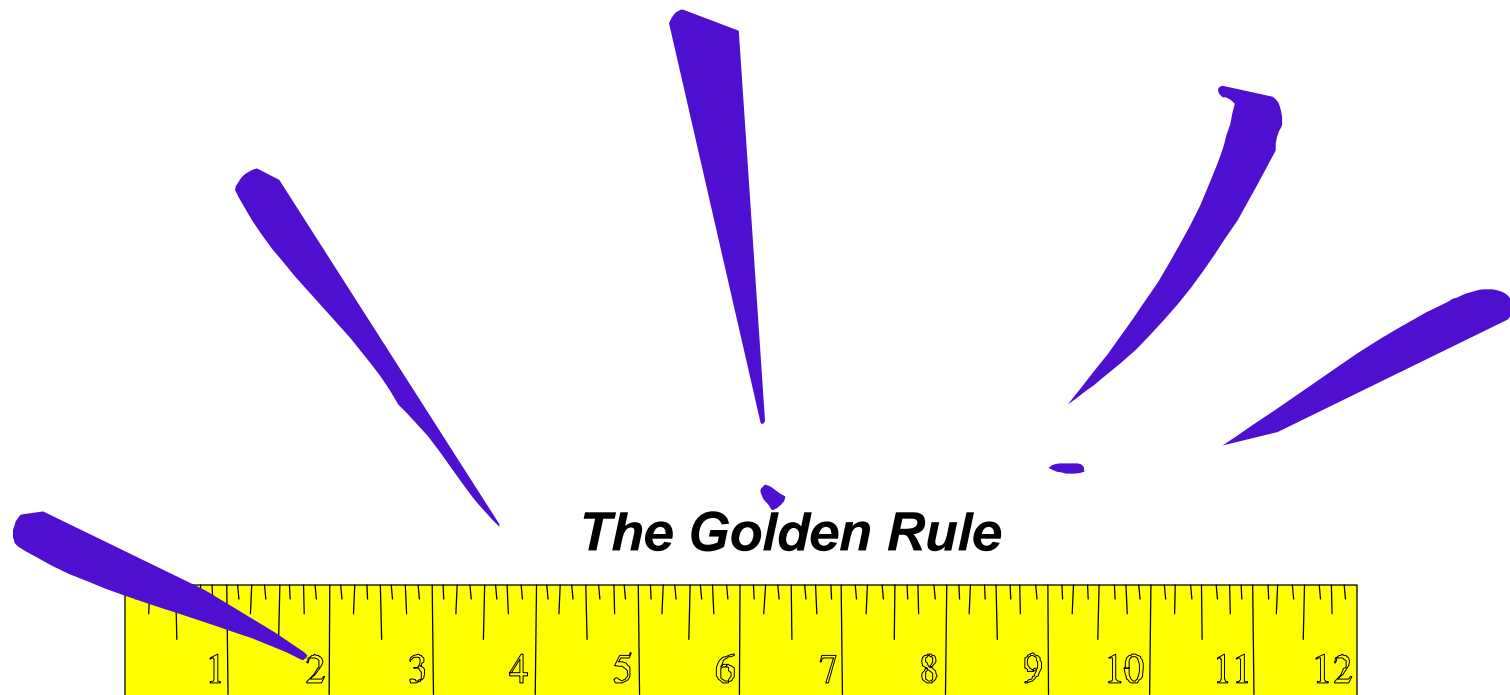
HIPAA Policies

- **Permitted uses**
- **Notices and information**
- **Business associates**
- **Patient rights:**
  - Accept restrictions?
  - When to deny access?
  - If amendment may be denied?
- **Administrative requirements**
  - Privacy officer
  - Training
  - Compliance reporting

What Technology?

The Most Important Technology

The Golden Rule

Standard:

"A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information"

Security*!*

37

Security Technology

Standard

Permitted uses and disclosures

Minimum necessary

Accounting for disclosures

Technology

Authorization control Encryption

Access control

Entity authentication Audit trail

Other Technology

Standard

De-identify

Restrictions

**Consents
Authorizations**

Technology

Algorithm

Flags

**Document imaging
Electronic signature**

Contact

Margret Amatayakul

Margret\A Consulting, LLC

Schaumburg, IL

Tel. 847-895-3386

MargretCPR@aol.com

www.Margret-A.com