

# **HIPAA Policies, Procedures and Training**

---

Margret Amatayakul, RHIA, CHPS, FHIMSS  
President, Margret\A Consulting, LLC



Steven S. Lazarus, PhD, FHIMSS  
Boundary Information Group, President



Paul T. Smith  
Davis Wright Tremaine LLP

# Privacy Training

---

## The Regulation

*“A covered entity must train all members of its workforce on the policies and procedures with respect to PHI required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function.”*

(45 CFR 164.530(b))

# Deadlines

---

- ◆ Training must be provided:
  - ❖ No later than April 14, 2003 (2004 for small health plans)
  - ❖ To new hires within a reasonable period
- ◆ Retraining must be provided
  - ❖ After change in job functions
  - ❖ After change in policies and procedures

# Documentation

---

- ◆ Training must be documented--
  - ❖ Maintained in written or electronic form for 6 years.
- ◆ What is not required
  - ❖ Employee acknowledgment or certification
  - ❖ Refresher training

# What The Regulation Requires

---

- ◆ The security requires security awareness and training for all personnel, including management, with the following “addressable” implementation specifications:
  - ❖ Periodic security reminders
  - ❖ Education on virus (“malicious software”) protection
  - ❖ Log-in monitoring
  - ❖ Password management
  - ❖ (45 CFR 142.308(a)(5))

# Who Must be Trained?

---

## ◆ Privacy

### ❖ Workforce must be trained

- Employees
- Volunteers
- Students
- Independent contractors with assigned workstations (if CE chooses)
- Occasional workers

### ❖ What about others?

- Medical staff
- Business associates

# Who Must be Trained?

---

## ◆ Security

- ❖ Was employees, agents and contractors, now just workforce (including management).
- ❖ Role-based training optional.
- ❖ Contractors must be aware of security policies, but do not need training.

# Policy and Procedure Training

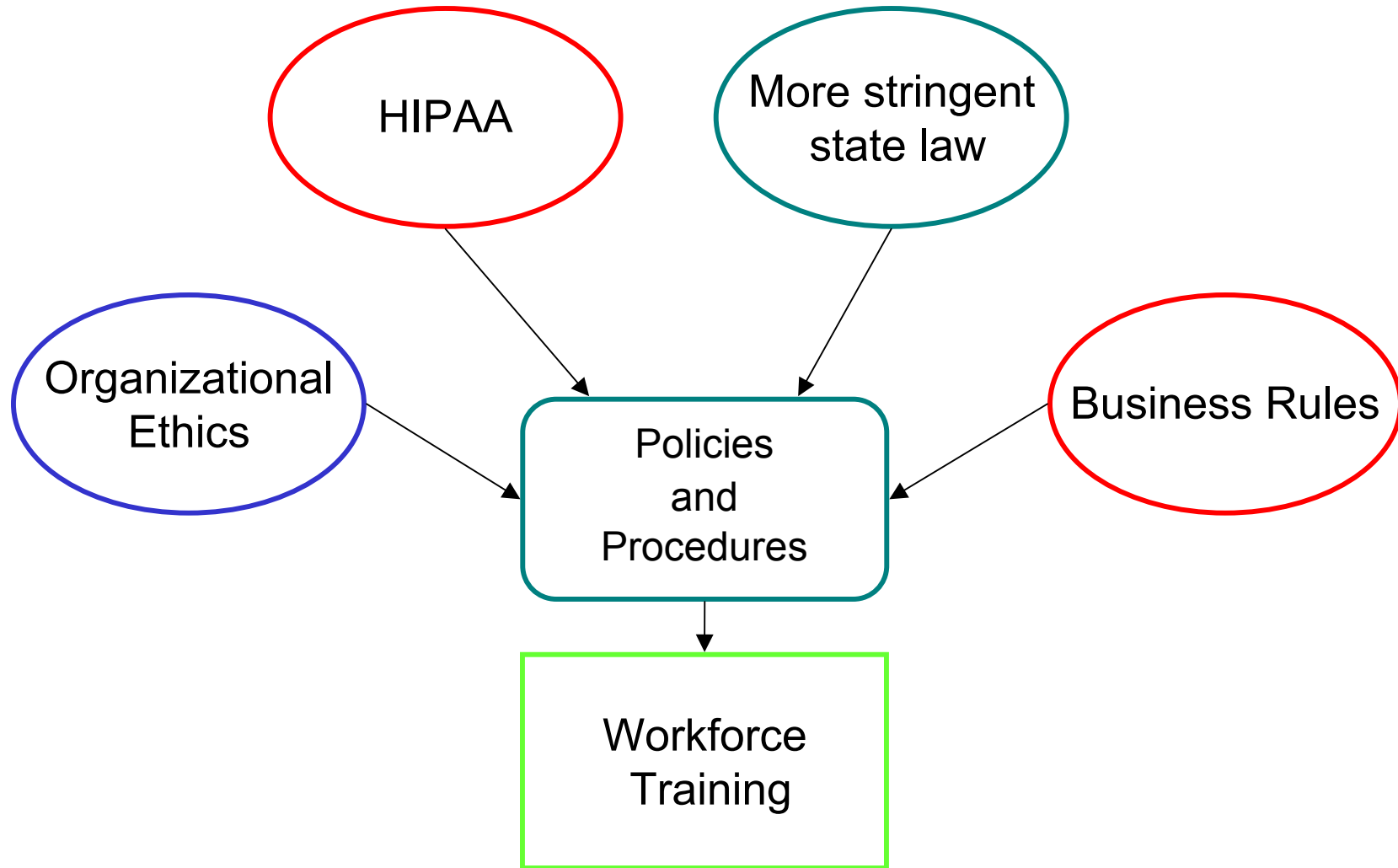
---

- ◆ Responsibility of Privacy Official is “development and implementation of the policies and procedures of the entity.”
- ◆ Cover—
  - ❖ Privacy administration
  - ❖ Physical protection
  - ❖ Technical safeguards
  - ❖ Use and disclosure
  - ❖ Sanctions and mitigation
  - ❖ Individual rights



# Policy and Procedure Development

---



# Policy and Procedure Development

---

- ◆ A HIPAA-Based Policy:

“We restrict the use and disclosure of all individually identifiable health information. Individually identifiable health information is information that identifies or could be used to identify an individual, and that contains information about the individual’s health condition or health care, including payment for health care.”

- ◆ An Alternative:

“We treat all health care related information as confidential, whether or not it identifies an individual, or could be used to identify an individual.”

# Policy and Procedure Training

---

HIPAA Education

Privacy Awareness Training

Role-Based  
Policy and Procedure Training

# Requirements

---

- ◆ Flexible and scalable
- ◆ You decide content and delivery
  - ❖ Classroom instruction
  - ❖ Videos
  - ❖ On-line training
  - ❖ Handbooks
- ◆ HHS says one hour per employee, on average

---

# **Training Case Studies: What Works and What To Watch Out For**

---

**Margret Amatayakul, RHIA, CHPS, FHIMSS  
President, Margret\A Consulting, LLC**

# Organization

---

- ◆ **Senior Management Oversight**
- ◆ **Delivery Network Oversight**
- ◆ **Focused Committees:**
  - ❖ **Privacy**
  - ❖ **Security**
  - ❖ **EDI**
  - ❖ **Education**
- ◆ **Coordination through central project manager**
- ◆ **Monthly meetings to address issues**

# Monthly Reporting

---

- ◆ **Project Status Summary**
  - ❖ **Task**
  - ❖ **Due Date**
  - ❖ **Percentage Complete\***
  - ❖ **On Target (Y/N)**
- ◆ **Accomplishments**
- ◆ **Next Steps**
- ◆ **Issues/Concerns/Barriers**

# \* Percentage Complete

---

**100% = Final Draft Approved**

**95% = Summary to Education Committee**

**90% = Operational Issues Resolved and  
Second Draft Completed**

**75% = Work Flow and Forms Developed**

**50% = First Draft Completed**

**35% = First Draft Submitted for Review**

**25% = Document Template Reviewed and  
Questions Generated**

**10% = Document Template Received**

**0 = Not Started**



# Policy & Procedure Templates

Title: <i>Use and Disclosure of PHI for Marketing</i>		Number:
Originator:	I	
Date(s) Reviewed:	I	

## SUMMARY:

[Name of Provider] requires that all communications use this policy if dates, a justification for use and marketing and a plan for obtaining authorization and approved by [specify position or group, such as Vice President of Operations]. All communications are within the scope of this policy.

## SCOPE OF POLICY AND PER

Portability of data should be maintained. The policy applies to all products and services of the patient or for use or recommend alternative treatment patient.

## TERMS

Disclosure - release, transfer, use of health information outside of the c

Marketing - is

1. A communication about communication to purch

c. Is for case management, coordination or direction of commercial alternative treatment, therapies, healthcare providers, or settings of care to an individual.

2. An arrangement that involves protected health information for the generation, for the of, or otherwise that

Procedural information that is or

Use - with application, the employment of such information that

## POLICY

- I. [Name of Provider] will obtain authorization for disclosure of protected health information for any marketing communications we purchase through a business associate to perform our business or make available to third parties for marketing communications about products or services.
- II. Any marketing communication must be approved by [specify position or group, such as Information Privacy Official or Vice President of Operations]. Approval will be based on a formal justification for use and disclosure of protected health information for purposes of the marketing and plan for obtaining authorizations from patients for such marketing communication.

## PROCEDURE

- I. In establishing a justification for a marketing communication, cost/benefit factors must be explained, including (and in order of priority):
  - A. The benefit to the patient.
  - B. Any potential exposure (loss of goodwill) with regard to our relationship with our patient.
  - C. The direct cost of obtaining an authorization from each patient.
  - D. The direct financial benefit to the organization.
- II. In developing a plan for a marketing communication, the following processes must be established:

Make Operational Decisions

Educational Summary

Request for Access or Disclosure for Treatment and Disclosure of Treatment and Information

# Forms

PATIENT NAME: \_\_\_\_\_

DATE OF BIRTH: \_\_\_\_\_ FORMER NAME: \_\_\_\_\_ MEDICAL RECORD #: \_\_\_\_\_

ADDRESS: \_\_\_\_\_ CITY: \_\_\_\_\_ STATE: \_\_\_\_\_ ZIP: \_\_\_\_\_

DAY PHONE: \_\_\_\_\_ EVENING PHONE: \_\_\_\_\_

I hereby authorize [Name of myself/you] to disclose my protected health information as indicated below to:

Mail to  Hold for pickup by:

NAME: \_\_\_\_\_ RELATIONSHIP: \_\_\_\_\_

ADDRESS: \_\_\_\_\_ CITY: \_\_\_\_\_ STATE: \_\_\_\_\_ ZIP: \_\_\_\_\_

PHONE: \_\_\_\_\_ FAX: \_\_\_\_\_

INFORMATION TO BE RELEASED:

DATES: \_\_\_\_\_

Discharge Summary  
 History & Physical Exam  
 Progress Notes  
 Lab Reports  
 X-Ray Reports  
 Medication Records  
 Detailed Bill  
 Other (specify content and dates): \_\_\_\_\_

I specifically authorize the release of information relating to:

Substance abuse (including alcohol/drug abuse)  
 Mental health or behavioral health  
 HIV related information (AIDS related testing)

\_\_\_\_\_  
 SIGNATURE OF PATIENT OR PERSONAL REPRESENTATIVE DATE: \_\_\_\_\_

PURPOSE OF DISCLOSURE:

Changing physicians  Consultation  Insurance/Workers' Compensation  School  Research  At request of individual  
 Legal (specify) \_\_\_\_\_  
 Other (specify) \_\_\_\_\_  
 For personal access (specify):  Copy  Inspection  Summary

ACKNOWLEDGEMENT OF UNDERSTANDING:

I understand the expiration date of this authorization is \_\_\_\_\_  
 I understand that I may revoke this authorization at any time by notifying the provider in writing, unless otherwise stated in advance upon it.  
 I understand that information may be disclosed pursuant to this authorization may be protected by Federal privacy laws.  
 By authorizing this use of my information, there will be no conditions placed on the use of my information.  
 I understand that I am authorized to authorize a use or disclosure that I will get a copy of my information within 30 days. If I am not provided access or information within 30 days, I will request a review of any denial of access other than those made in accordance with applicable law. The cost of preparing and mailing copies, superseding my request for a summary except for review, payment, and operation.

DATE: \_\_\_\_\_ RELATIONSHIP: \_\_\_\_\_  
 DATE: \_\_\_\_\_ IDENTIFIED: \_\_\_\_\_

FOR OFFICE USE ONLY

PHYSICIAN: \_\_\_\_\_ DIVISION REQUESTED: \_\_\_\_\_ DATE FILLED: \_\_\_\_\_

REASON FOR DENIAL WITH YOUR REQUEST BECAUSE:

The information you request was determined by [Name of Provider] to be withheld in accordance with applicable law.  
 Access is denied because such access may be harmful to you or someone else. You may request review of denial by contacting our Information Privacy Official.  
 Access is denied for periods of the record or the denied a summary or periods of the record is supplied instead.

YOU REQUEST FOR REVIEW HAS BEEN PROCESSED:

An independent licensed health care professional has  confirmed the need to deny your request  recommended provision of access, as supplied.  
 If you have any further questions with this complaint, please contact our Information Privacy Official. You may also request information about filing a complaint with the Secretary of Health and Human Services from our Information Privacy Official.

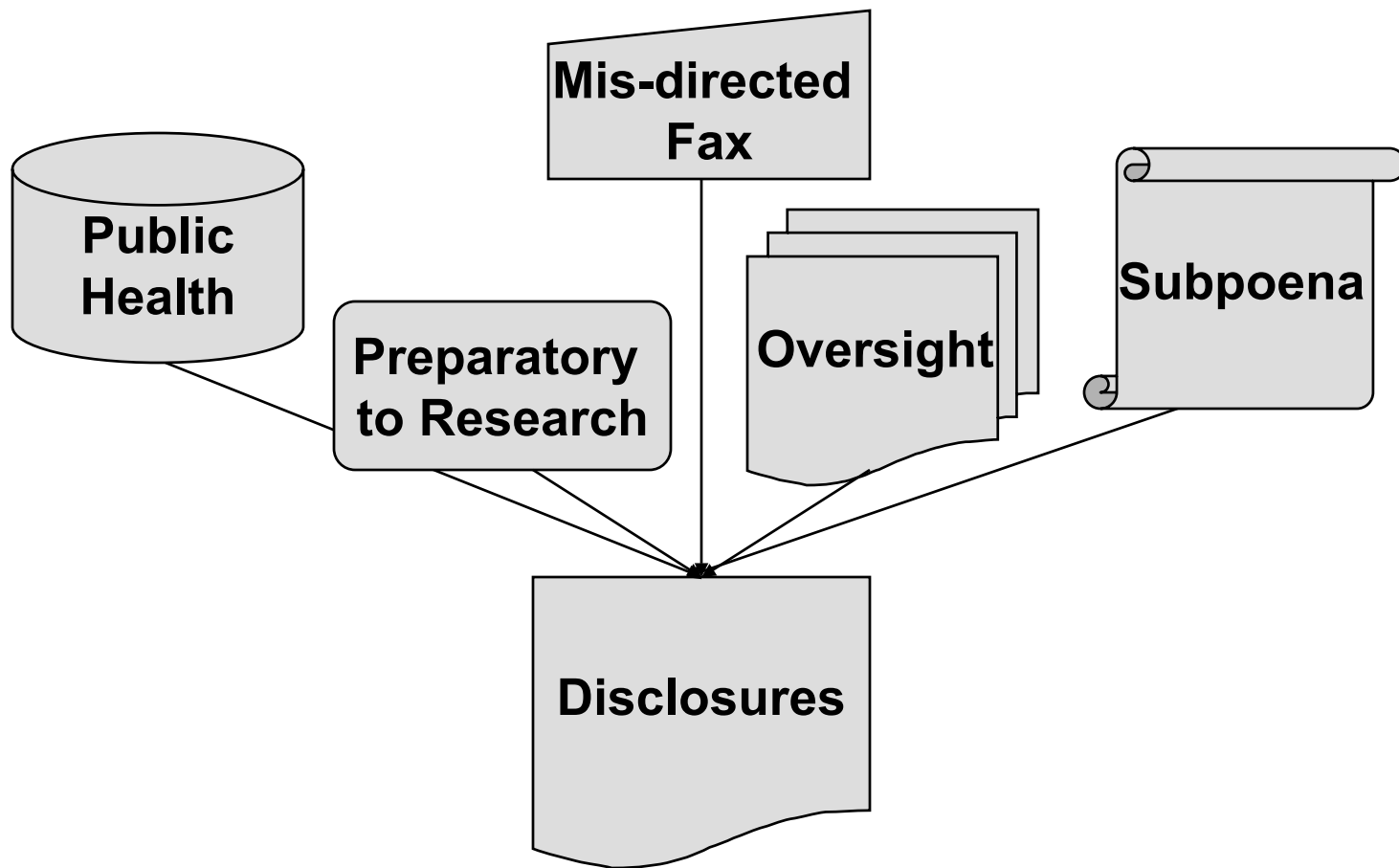
To contact our Information Privacy Official, call or write [apply for name, address, and phone number and e-mail/web site].

Structure Options

“For Office Use Only”

# Work Flow

## Accounting for Disclosures



# Examples

Marketing	Not Marketing Communication
<p><b>A communication about product or service that encourages recipients to purchase or use product, unless . . .</b></p>	<p><b>Covered entity describes health-related product or service, or makes a face-to-face communication/ provides promotional gift of nominal value.</b></p>
<p><b>Provider allows diaper company sales rep to visit new mothers.</b></p>	<p><b>Provider distributes diaper samples and/or coupons to new mothers.</b></p>
<p><b>Provider gives list of patients on certain medications to pharmaceutical company for them to market drugs</b></p>	<p><b>Providers gives sample drug, tells patient about certain drug, or sends brochure about certain drug to patients who would benefit from taking drug</b></p>
<p><b>Provider sells list of patients to a local community college for them to sell smoking cessation and weight loss programs.</b></p>	<p><b>Provider sends information about smoking cessation program it is providing to patients who are determined to be smokers.</b></p>

# Anticipate and Script

---

## ◆ If:

- ❖ Patient refuses to sign
- ❖ Patient refuses to accept
- ❖ Patient asks what this is
- ❖ Patient asks for restrictions

## ◆ Then:

- ❖ Check “no sign” in computer
- ❖ Check “refused” in computer
- ❖ Explain that this is ...
- ❖ Provide Request for Restrictions Form and refer to Supervisor

# Gaining Approval

**Policy Name:**

**Type:**

**Number:**

**Executive Sponsor:**

**Status:**  New  Revision **Date:**

**Summary:** *Essence of policy and procedure in two to three sentences.*

**Impact:**

**Affected Components:** *Identifies classes of workers/units most impacted.*

**Operations:** *Critical elements that positively and/or negatively change the way the organization functions.*

**Financial:** *Operational and capital cash outlays required as well as any return on investment and/or loss avoidance that can be quantified.*

**Risk Assessment:**

*Briefly describes the risk of not implementing the policy and procedure, and the residual risk after implementation.*

**Reason:** *Describes why the policy and procedure is created/revised.*

# Decision Table

<b>Request for Restriction</b>	<b>Yes</b>	<b>No</b>	<b>Document</b>
<b>Mail EOB to alternative address</b>	<b>X</b>		<b>Billing System</b>
<b>Appointment Reminder</b>	<b>X</b>		<b>PMS</b>
<b>Restrict Use to Dr. Smith Staff</b>	<b>X</b>		<b>EMR</b>
<b>Restrict Use by Dr. Smith Nurse</b>		<b>X</b>	
<b>Self Pay</b>	<b>Refer to Bus Mgr</b>		<b>Billing System</b>

# Target Training

	A	B	C	D	E	F	G
1	Keywords/ Education-Training-Awareness Content	Core Content for All Workforce	Additional General Information About Topics				
2			Nursing Personnel as Designated by Departments	Other Caregivers as Designated by Departments	Non-Clinical Administrative/ Financial	All Medical Staff	Board of Directors Senior Mgt
3	<b>HIPAA in General</b>						
4	Administrative Simplification	X					
5	Affiliated Covered Entity						X
6	C-I-A (Confidentiality-Integrity-Availability)	X					
7	Compliance	X					
8		X					
9					*		X
10							X
11			X	X	X		X
12					*		X
13	Health Information Exchange				*		X
14	Hybrid Entity						X

**Categorize by:  
Keywords or  
Policies &  
Procedures**



# Organize Training

---

## ◆ Standards

- ❖ Integrate policies and procedures
- ❖ Refer to/link to policies and procedures

## ◆ Notice of Privacy Practices

- ❖ Topics
- ❖ Categories

## ◆ General Topics

- ❖ Avoid focusing too much on HIPAA
- ❖ And not enough on your operations

# Training Examples

## How Do We Share PHI for TPO?

The XXXXXX family of providers, including XXXXXXXXXXXXXXX Hospital and XXXXXX Hospital, may share your health information among each other and with the physicians on our respective medical staffs for purposes of providing you with treatment, obtaining payment for health care, and for other purposes. Examples of sharing in operations are described below.

HIPAA permits us

**T**reatment = providing care, including with a third party

**P**ayment = determining collections, reviewing reporting relative to

**O**perations = conducting qualifications of personnel, planning, general administrative

### Our Values

**Patient Confidentiality** is part of our **SERVICE EXCELLENCE** Expectations

- Considerate
- Attentive
- Responsive
- Empathetic

Based on NOPP

Explains Specific Policy

# CARE

## TRANSMISSION/RECEIPT OF PHI VIA FAX

▲ Fax only information permitted by our policy:

- ◆ When PHI is not accessible through our information systems
- ◆ Mail or courier will not meet immediacy of need

Take special precautions for faxes with highly sensitive information (e.g., HIV, mental health, substance abuse)

Take reasonable steps to ensure faxes are transmitted to correct destination

Always use a fax cover sheet with our confidentiality notice

- ◆ Always use autodial, check display, check transmission report

▲ In the event of a misdirected fax:

Incorporates Provider's Own Values (Privacy is not new!)

# What to Watch Out For!

---

Does every one need to be trained in every thing?

But don't leave out critical staff!

- ◆ It is easy to create policies and procedures that reflect the rules,
  - ❖ It is more difficult to create policies and procedures that reflect how things will actually work in your environment
- ▶ It is easy to buy, or even develop, training materials that are generic,
  - ❖ It is more difficult to efficiently and effectively incorporate your specific policies and procedures into the training
- ▶ It is easy to plan a massive training roll out,
  - ❖ It is more difficult to achieve full compliance on training,
  - ❖ Let alone get everyone to understand what to do,
  - ❖ It is even more difficult to ensure that compliance lasts
- ◆ Although the Privacy Rule does not require awareness building or reminders, this is critical for ongoing compliance

---

# Advanced Strategies in Complying with the HIPAA Workforce Training Requirement

---



*Steven S. Lazarus, PhD, FHIMSS*  
*Boundary Information Group, President*  
*Train for Compliance, Inc., Vice Chair*  
*Workgroup for Electronic Data Interchange*  
*(WEDI), Past Chair*

# Achieving Effective Privacy and Security

---

- ◆ Need good Security to achieve Privacy
- ◆ Privacy Regulation requires Security
- ◆ Reminders, periodic training, and “breach monitoring” reporting and management will be needed to achieve effective Privacy
- ◆ Need to train the workforce on the organization’s policies and procedures for Privacy and Security

# Policies and Procedures

---

- ◆ Privacy Administration
- ◆ §164.530(i) and 164.520(b)
- ◆ Process for developing, adopting and amending of privacy policies and procedures, making any necessary changes to the Notice of Privacy Practices, and retaining copies

# Policies and Procedures

---

- ◆ Including overriding principles (policy)
- ◆ Detail practices
  - ❖ Identify responsible individual or department
  - ❖ Define specific operational processes
  - ❖ Require enough detail so that the workforce knows what to do
  - ❖ Develop to fit the clinical and business operations of the covered entity
- ◆ Must not just repeat or summarize the Regulations
- ◆ Privacy policies and procedures must reflect state laws that are more restrictive

# Examples of Forms for Policies and Procedures

---

- ◆ Notice of Privacy Practice acknowledgement form
- ◆ Notice of Privacy Practice non-acceptance form
- ◆ Inventory of Business Associates
- ◆ Patient Authorization
- ◆ Certificate for completing training
- ◆ Incident Report



# Organizing Policy and Procedure Development and Revision

---

- ◆ Chief Information Privacy Official
- ◆ Chief Information Security Official
- ◆ Workgroups
  - ❖ Privacy
  - ❖ Security
  - ❖ Transactions, Code Sets and Identifiers
  - ❖ Education/training

# Policy and Procedure Development Process

---

- ◆ Gap analysis of existing policies and procedures
- ◆ Identify needed changes
- ◆ Develop new/revised policies and procedures
- ◆ Approve policies and procedures
- ◆ Replace former policies and procedures
- ◆ Train the workforce on the policies and procedures

# Training Issues and Options

---

- ◆ Define workforce categories
  - ❖ Few workforce categories
    - Easy to administer
      - Assign workforce to courses
    - Less customization to create and maintain
  - ❖ Many workforce categories
    - May be difficult to administer
      - Complex management of workforce to training content choices
    - Potential to highly customize content to workforce categories

# Training Issues and Options

---

## ◆ Practical Issues

- ❖ Identify source of workforce lists, identifications and passwords
- ❖ Include employees, physicians, volunteers, long-term contract renewal (e.g., Medical Director in a health plan)
- ❖ Use Human Resource application if capable
  - Names
  - Job categories
  - Identifications and passwords from another source
- ❖ Keep passwords and identifications secure

# Training Issues and Options

---

- ◆ Tests

- ❖ Use to document learning for compliance

- ❖ Set passing score

- ◆ Consider Continuing Education credits (can not change content significantly and maintain credits)

# Training Issues and Options

---

## ◆ Training Options

### ❖ In person – classroom

- Can customize
- Questions and answers addressed by trainer
- Difficult to schedule for new workforce members
- Can use paper or automated testing

# Training Issues and Options

---

- ◆ Video or Workbooks
  - ❖ Can not customize
  - ❖ No questions and answers
  - ❖ Need VCRs and/or supply of Workbooks

# Training Issues and Options

---

## ◆ E Learning

- ❖ May be able to customize
- ❖ Limited questions and answers
- ❖ Flexible schedule for training for current and new workforce
- ❖ Can integrate training with organization's policies and procedures
- ❖ There may be technological barriers depending on delivery mode
- ❖ Automated testing and learning reinforcement



# Training Cost

---

## ◆ Cost/Budget

### ❖ Product

- Fixed price
- Per course per person
- Maintenance

### ❖ Customized setup

- Policies and Procedures
- State Law pre-emption for Privacy
- CEs
- Assign courses to individuals

# Training Cost

---

- ◆ Workforce training time
  - ❖ Salaries and benefits
  - ❖ CE offset
- ◆ CE value/budget
- ◆ Technology
  - ❖ Several VCRs, monitors, and rooms, website
  - ❖ Support – internal and external
- ◆ Administrative
  - ❖ Record keeping
  - ❖ Management

# Setup Issues

---

- ◆ Setup Time and Resources

  - ❖ Assignment of internal staff/outsource

  - ❖ Initially may require dedicated staff, rooms, and equipment

- ◆ Pilot Training

  - ❖ Evaluate learning

# Achieving Effective Privacy

---

- ◆ Need good Security to achieve Privacy
- ◆ Privacy Regulation requires Security
- ◆ Reminders, periodic training, and incident monitoring” reporting and management will be needed to achieve effective Privacy

# Contact Information

## ◆ Paul Smith

❖ Davis Wright Tremaine, LLP

❖ Tel. 415-276-6532 ❖ PaulSmith@dwt.com ❖ www.dwt.com

## ◆ Margret Amatayakul, RHIA, CHPS, FHIMSS

❖ Margret\A Consulting, LLC

❖ Tel. 847-895-3386 ❖ MargretCPR@aol.com ❖ www.Margret-A.com

## ◆ Steve Lazarus, PhD, FHIMSS

❖ Boundary Information Group

❖ Tel. 303-488-9911 ❖ SSLazarus@aol.com ❖ www.boundary.net