



# HIPAA Common Practices: Small vs. Large Entities

---

Roy Rada, M.D., Ph.D.  
Univ. Maryland Baltimore Co.  
rada@umbc.edu



# What about best practices?

---

Best practices should be

- quantifiably successful over a prolonged period and
- repeatable with modification in similar organizations.



# We are not there!

---

- Searched web for “HIPAA Best Practices”
- None were quantifiably successful
  - None were over time
  - None had been systematically reapplied



# Wanted

---

Practices that are

- Common and
- Compliant

The same for all entity types?



# Small treated like Large?

---

Average HIPAA expenditure 2001		
<100 beds	100 to 400 beds	>400 beds
\$3,000 per bed	\$900 per bed	\$300 per bed



# Recommend Different HIPAA Toolkits

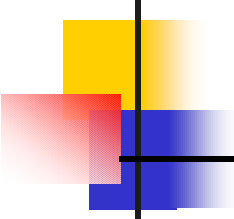
---

For small group  
physician practice

- 30 pages
- Self-contained
- Few hours of effort

For multi-hospital  
network

- Thousands of pages
- Requires extra tools
- Person years



# Outline of 30-page manual for small group physician practice

---

## Privacy

- Patient Rights
- Communication
- Administration
- Training

## Ecommerce

- Benefits
- Letter to Vendors
- Codes
- Delay Application



# Patient Rights Checklist

---

<i>Do you have?</i>	<i>Yes</i>	<i>No</i>
Consent		
Authorization		
Notice of Privacy Practices		
Access and Amend Policy		
Accounting and Restriction Policy		





# Example Consent Form

---

Name of Provider  
Patient Consent Form

Our Notice of Privacy Practices provides information about how we may use and disclose protected health information about you. You have the right to review our notice before signing this consent. As provided in our notice, the terms of our notice may change. If we change our notice, you may obtain a revised copy by \_\_\_\_\_. You have the right to request that we restrict how protected health information about you is used or disclosed for treatment, payment or health care operations. We are not required to agree to this restriction, but if we do, we are bound by our agreement. By signing this form, you consent to our use and disclosure of protected health information about you for treatment, payment and health care operations. You have the right to revoke this consent, in writing, except where we have already made disclosures in reliance on your prior consent.

\_\_\_\_\_  
Signature of Patient or Personal Representative

\_\_\_\_\_  
Name of Patient or Personal Representative

\_\_\_\_\_  
Date



# 1-Page Information Practices Notice

---

## **PROVIDER NOTICE OF INFORMATION PRACTICES**

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Uses and disclosures of health information:

We seek your consent to use health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive. You can revoke your consent.



# Physician Practice Policy on Access

---

## **Access Right**

We give you access to your health information whether we or our business associates hold that information and whether or not we were the source of the information. Exceptions to this access occur rarely, such as when the information is deemed dangerous. If we feel we need to deny access, we must provide an explanation. Sometimes you can contest this denial, and then we will have a third party review the situation.

You may request access verbally or in writing, and we will record your request in a log book. We typically have 30 days in which to provide the information. We will charge you the cost of reproducing and delivering the information; for photocopying this charge is \$0.20 per page.



# Communication Checklist

---

<i>Do you have policies for?</i>	<i>Yes</i>	<i>No</i>
Phone and face-to-face		
Email and fax		
Medical records		



# Email Policy

---

## **Ownership and User Privacy of E-Mail**

Use of electronic mail is a part of <ENTITY> business processes. All e-mail originating within or received into <ENTITY> is the property of <ENTITY>.

## **Confidentiality of Electronic Mail**

When e-mail is used for communication of individually identifiable health information, specific measures must be taken to safeguard confidentiality. These safeguards follow:



# Administration Checklist

---

<i>Do you have?</i>	<i>Yes</i>	<i>No</i>
Privacy Officer		
Business Associate Contracts		
Auditing		
Safeguards		
State pre-emptions		



# Business Associate Contract

---

- THIS CONTRACT is entered into on this \_\_\_\_\_ day of \_\_\_\_\_ between \_\_\_\_\_ ("ENTITY") and \_\_\_\_\_ ("ASSOCIATE").
- WHEREAS, ENTITY will make available to ASSOCIATE certain Information that is confidential and must be afforded special treatment and protection.



# Auditing

---

Disclosures based on Authorizations for Patient  
Named " \_\_\_\_\_ "

Date	To whom Sent	What was Sent	Purpose





# Training Checklist

---

Privacy Training			
Person's Name	Date Completed		
	Physician Essay	Staff Essay	Entire Manual



# Physician Awareness

---

- The independent physician in a small practice is challenged by budget reforms and legal minefields that make the practice of medicine not what it was in the good old days. The latest challenge comes in the form of HIPAA's Administrative Simplification provisions.



# Staff Training

---

All staff are involved in protecting health information. Staff should be aware of the penalties that could be levied against them by the Federal government. Fines reaching \$250,000 and imprisonment can be imposed on physicians, practice managers, receptionists, medical assistants, or nurses. Untrained staff may not realize that respecting privacy is important. All staff are required to undergo training on privacy.



# Ecommerce Checklist

---

Have you	Yes	No
Analyzed business efficiency?		
Checked vendor compliance?		
Determined code gap?		
Applied for delay?		



# Business Efficiency Spreadsheet

---

1. Number of claims per week: 215
2. Average claim value: \$191
3. Time to prepare a manual claim: 6 minutes
4. Time to prepare an electronic claim: 0.5 minutes
5. Staff cost per hour: \$14
6. Manual cost per year:  $\#1 * \#3 * \#5 * (1 \text{ hr}/60 \text{ min}) * (52 \text{ wks}/\text{yr})$   
= \$15,652.
7. Electronic cost per year:  $\#1 * \#3 * \#4 * (1 \text{ hr}/60 \text{ min}) * (52 \text{ wks}/\text{yr})$  = \$1,304.
8. Labor saving is  $\#6 - \#7 = \$14,348$ .
9. Bad debt now: 10 %
10. Bad debt after automation: 5%
11. Annual savings from debt change:  
 $\#1 * \#2 * (\#9 - \#10) * (52 \text{ wks}/\text{yr}) = \$106,769$ .



# Letter to Clearinghouse

---

Please explain:

- your timeline to address each of the transaction changes required by HIPAA and
- what you expect the practice to do in order to work effectively with you to achieve compliance with HIPAA?



# HHS Form for Delay

---

10. Please check the reason(s) that your organization will not be in compliance with the HIPAA standard for Electronic Transactions and Code Sets by October 16, 2002. Multiple boxes may be checked.
- Need more money
  - Need more staff
  - Need more information about the standards
  - Waiting for vendor(s) to provide software



# Conclusion on Physician Practice

---

- Simple
- Consistent with sound business
- Graspable handle on entire operation





# Large Entity

---

Compliance requires

- Many people
- Many deliverables

Examples of complexity:

- Staffing
- Project management
- Transactions
- Training

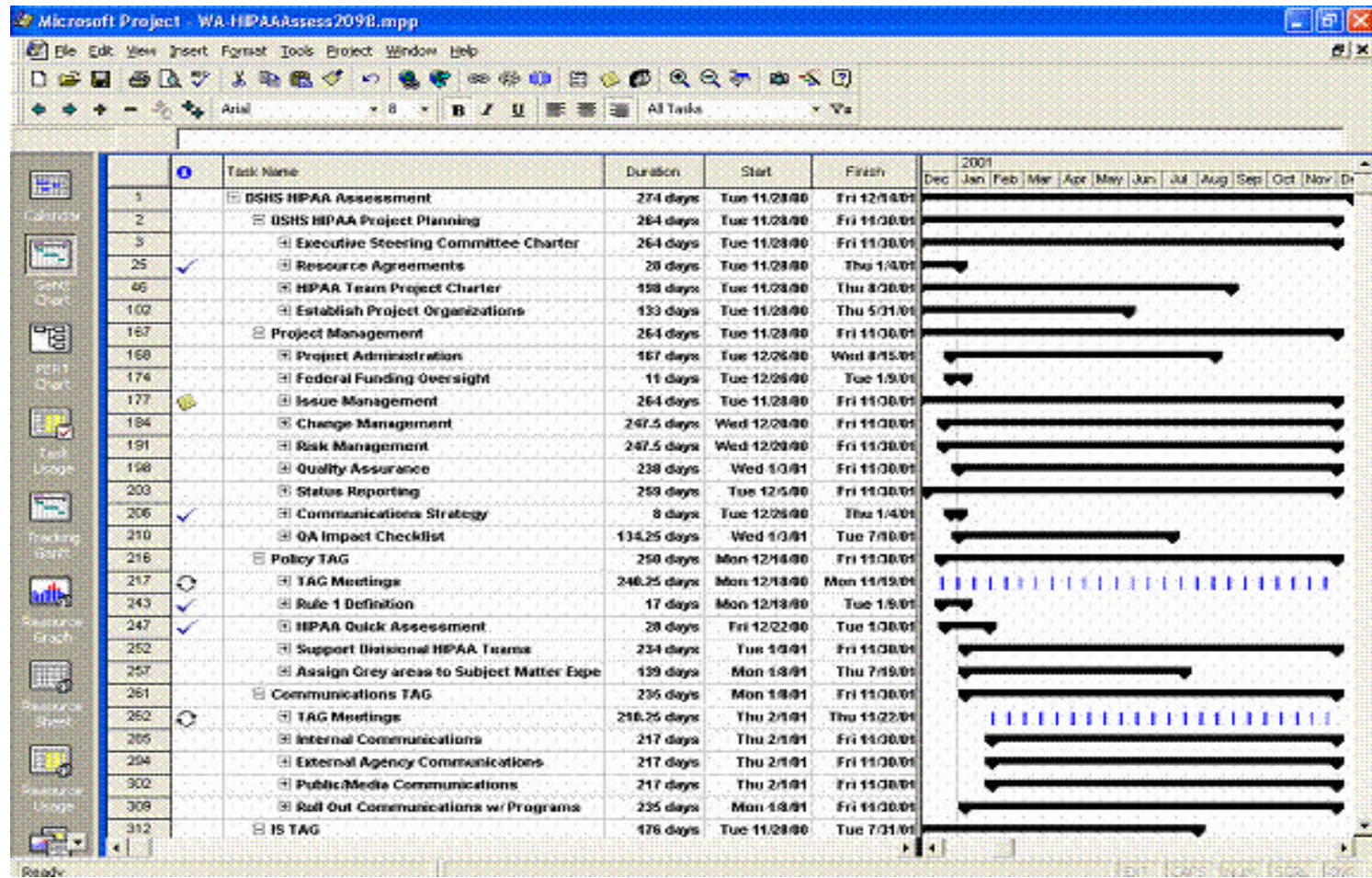


# Hospital Staffing

---

- Departments: administration, information systems, finance, legal, compliance, inpatient, ambulatory, medical records.
- Leadership: Chief Compliance Officer, Information Officer, Finance Officer, and/or Legal Counsel.

# Microsoft Project





# Transactions

---

You may

1. rely on clearinghouse,
2. translate on the border, or
3. internally integrate.

As go from 1 to 3 the short-term costs drop but long-term costs rise.



# Costs without Clearinghouse

---

- translators can be purchased for \$ tens of thousands but
- tailoring to work costs \$ hundreds of thousands, and
- an internal integration is \$ millions.



# Training

---

Section '§ 164.530 Administrative requirements' includes this sentence:

- (b)(1) Standard: training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.



# Roles to be Trained

---

Roles Ri in clinics plus health plan

- R1 Medical Doctors.
- R2 Medical Assistants.
- R3 Clinic Regional Administrator.
- R4 Claims Examiners.
- R5 Provider Information Analyst.
- R6 Application Operations Analyst.
- R7 Member Services Representatives
- R8 Authorizations Specialist.
- R9 Billing Representative.
- R10 Enrollment Representative.



# Content to Roles for Training

Privacy Rule Component  $P_i$  (like consent) to Role  $R_i$

---

Pi to Ri need-to-know of ++, +, 0										
	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10
P1	++	++	++	+	0	0	++	++	0	0
..										





# Conclusion on Large Entities

---

- Many roles.
- Many policy specifics.
- Much existing infrastructure to match.
- An opportunity to further harmonize or a big headache.



# Conclusion

---

- Common practices are appearing.
- What works differs from small to large entities.
- Entities should share and define the standard for their entity type.