Privacy in 24 Hours:
or 140,000 Hours

Roy Rada, M.D., Ph.D.
Prof. at UMBC, rada@umbc.edu
Publisher of www.hipaa-it.com

Start Small

For 2-doctor office with 4 assistants, privacy manual

- is 25 pages,
- is self-contained, and
- takes 24 person hours to implement.

Then scale to large.

24 Hour Compliance

- Phase 1: Executive reads awareness essay & passes manual to office manager – 1 hr.
- Phase 2: Office manager studies current policies, and information flows – 5 hrs.
- Phase 3: Policies tailored and business associates contacted – 3 hours

24 Hours (con't)

- Phase 4a: Everyone trained – 5 hours
- Phase 4b: Procedures implemented – 3 hours
- Phase 4c: Business associate contracts signed – 4 hrs.
- Phase 4d: Administration by office manager – 3 hrs.

Total 24 Hours

Privacy Manual for small entity

- Patient Rights, Communication, Administration

Patient Rights Checklist: Do you have?	*Yes*	*No*
Notice of Privacy Practices		
Authorization		
Access and Amend Policy		
Accounting and Restriction Policy		

Notice

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED … AND HOW YOU CAN GET ACCESS …

……

[Further details is 3 pages]

###

Acknowledgement of receipt of Notice of Privacy Practices:

Signature: _____

Communication Checklist

Do you have policies for?	*Yes*	*No*
Phone and face-to-face		
Email and fax		
Medical records		

Medical Record

Role	Information
Chief	Everything
Medical Assistants	Health
Receptionist	Scheduling
Information Manager	Billing

Administration Checklist

Do you have?	*Yes*	*No*
Privacy Officer		
Business Associate Contracts		
Accountability		
Safeguards		
State pre-emptions		
Training		

Executive Awareness

Awareness essay is 1,000 words.

- Gentle
- Reasonable
- Solution-filled

Begins: The executive in a small facility is challenged by budget reforms and legal minefields. The latest challenge comes in the form of HIPAA's Administrative Simplification provisions.

Tables

5 electronic or paper tables could accommodate the range of expected behavior documentation.

Exceptional Disclosures for John Doe			
Date	To whom Sent	What was Sent	Purpose

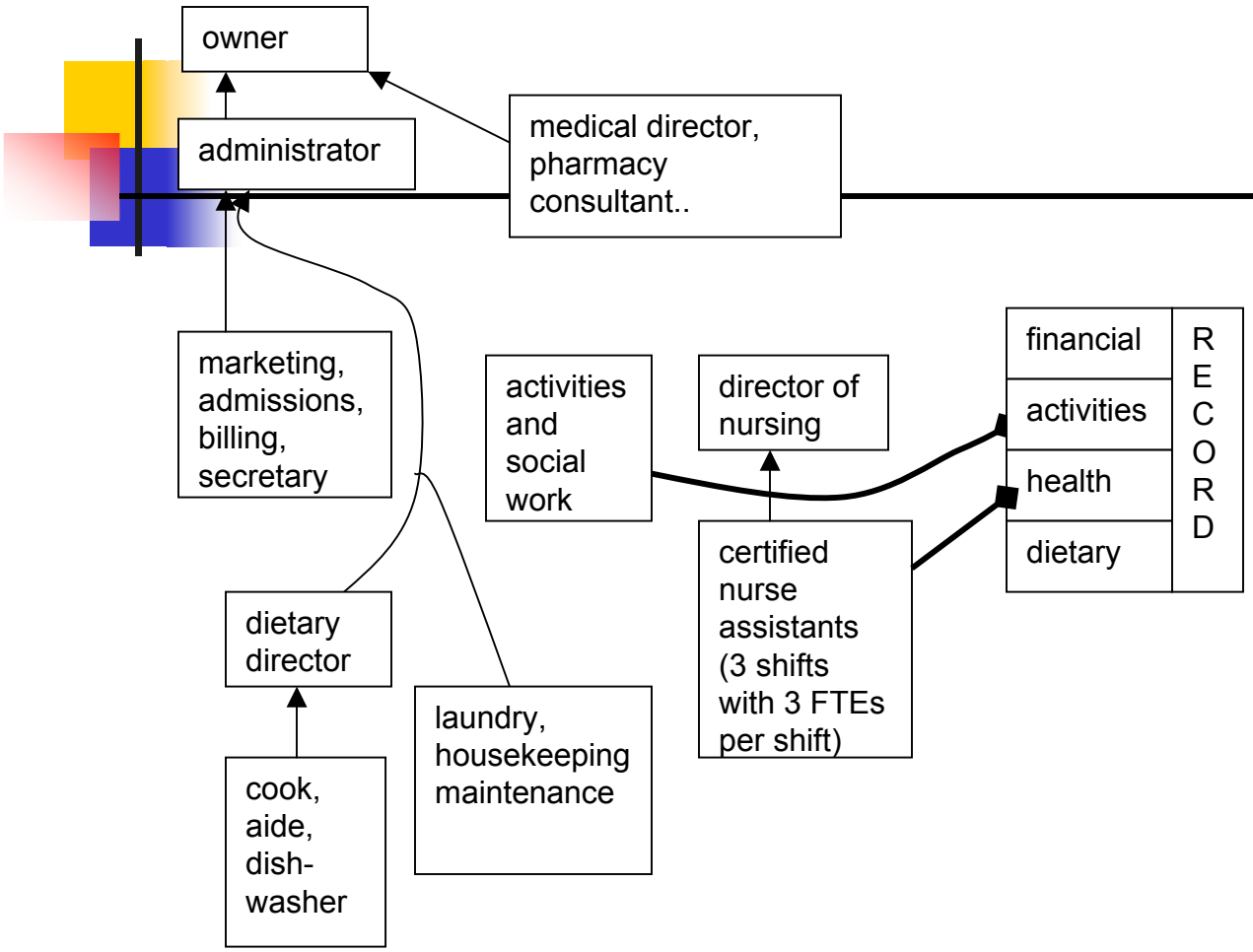
Requests

Requests for access, amendment, or accounting of disclosures. ONE TABLE FOR CENTRAL OFFICE (not in each patient record)			
Patient Name	*Date of Request*	*Date Satisfied*	*Details of Request*

As Entities Get Larger

- More roles.
- More policy specifics.
- More existing infrastructure to match.
- An opportunity to further harmonize or a bigger headache.

Example: 48 Hours for Nursing Home



Implementation time:
Chief: 1 hour,
Facility administrator: 13 hours,
34 other staff: 1 hour each.
Total time commitment of 48 hours.

Model

label	symbol	formula
parts per entity	n	
subparts per part	m	
employees per subpart	k	
total employees	emp	n*m*k
Privacy Officer Hours in a month	POmonth	.04*emp+2
CEO awareness	CEO	.0004*emp+1

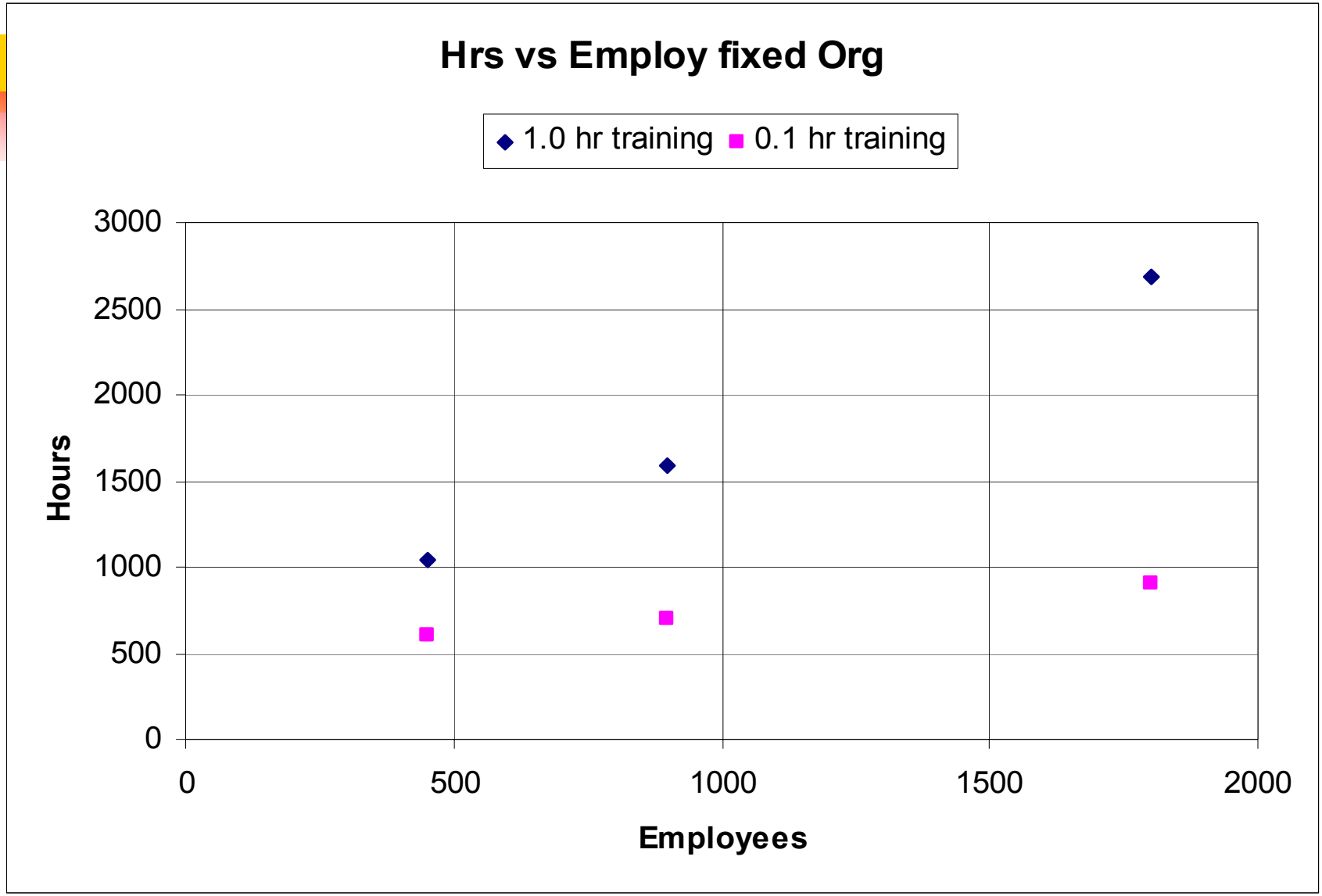
Model (con't)

Phase 1	CEO + ((n+m) *5)
Phase 2	5*(n*m)+POmonth
Phase 3	5*(n*m)+POmonth
Phase 4 training	1*emp+0.1*emp
Phase 4 procedures	n*5 + m*3
Phase 4 BA	(n+m)*8
Phase 4 admin	POmonth

Economies of scale

- 'organizational complexity' = n*m.
- organizational complexity at 30
  - employees from 450 to 900 to 1800 →
  - hour cost from 1,042 to 1,590 to 2,690.
- employees at 900
  - organizational complexity from 2 to 30 to 450 →
  - hour cost from 1,175 to 1,591 to 6,355.
- If 100,000 employees, then 145,000 hours.

Total Compliance Hours Halved by Reducing Training



Maintenance Costs

- 1-year Maintenance is a small fraction of Implementation Cost.
- Annual Maintenance Cost is approximately 0.1 of number of employees.

Risk Analysis

Threats	Remedies							
	I2	I3	I4t	I4p	Mr	Mc	Mp	Mt
Recipe	10	20	60	20	90	10	40	20
Leak	30	10	30	10	10	50	30	20
Audit	60	30	10	80	30	50	20	50
benefit	2.4	1.5	2.9	2.5	3.6	2.8	2.5	2.2
cost	224	224	1980	74	23	39	7	86

I=Implement and M=maintain. I2=collect information, I3=tailor policies, I4t=train, I4p=privacy office, M4=rights, Mc=communicate, Mp=privacy officer. Threats are Recipe, Leak, and Audit. Note: implementation training has worst cost/benefit ratio.

Conclusion

- Privacy compliance should be simple
- For small entity can be 24 hours
- Generally, training is the lion's share of implementation
- Maintenance is low cost but best value.