702 - UNIQUE CHALLENGES FOR HIPAA COMPLIANCE WITHIN A UNIVERSITY HYBRID ENTITY:

HOW TO MANAGE PRIVACY REQUIREMENTS IF YOU DO NOT HAVE AN AMC

HILA BERGER, *COMPLIANCE OFFICER, MONTCLAIR STATE UNIVERSITY*

1

OBJECTIVES

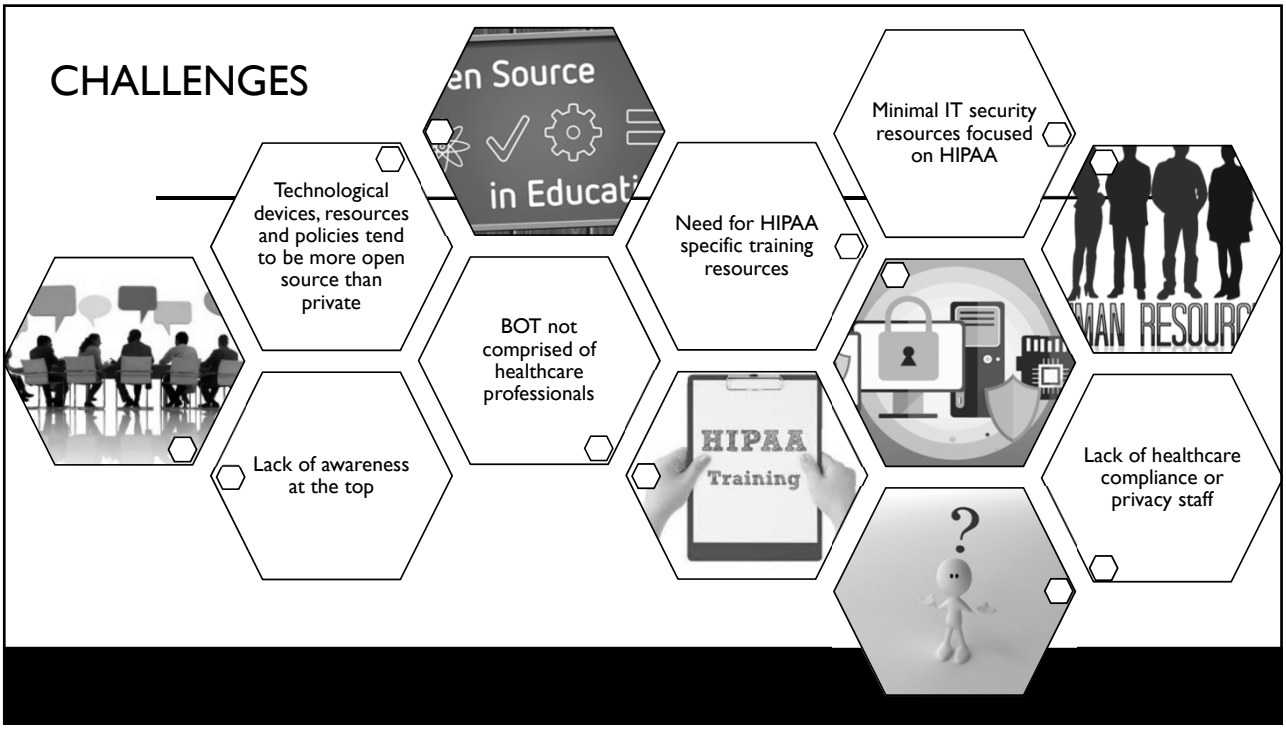
- Explore unique challenges in ensuring privacy when the culture of an organization is not healthcare based
  - Designating as a Hybrid entity
- Review case studies
  - Hybrid status ended in an OCR settlement
- How to shift privacy culture including Practical solutions for education and maintaining privacy

2

CHALLENGES IN HIGHER ED WITH NO AMC

3

CHALLENGES



4

DESIGNATION AS HYBRID ENTITY

5

DESIGNATION AS A HYBRID ENTITY

- Must be a formally approved document
  - Reviewed by Counsel
  - Approved by President or BOT
- Becomes a shield against potential problems
- Reduces risk of non-compliance and exposure to penalties
- Removing certain non-covered entities from HIPAA oversight
  - Example: University Student Psychological services clinic; Employee health services

6

HYBRID ENTITY AND DESIGNATION OF UNIVERSITY TRAINING CLINICS (WISE, R. A., KING, A. R., MILLER, J. C., & PEARCE, M. W. (2011). WHEN HIPAA AND FERPA APPLY TO UNIVERSITY TRAINING CLINICS. *TRAINING & EDUCATION IN PROFESSIONAL PSYCHOLOGY*, *5*(1), 48–56. HTTPS://DOI.ORG/10.1037/A0022857)

Applies when:

1. The University Training Clinic transmits protected health information electronically as part of a "covered transaction";
2. If the information pertains to a non-student, then the Transaction, Security, and Privacy Rules will apply;
3. If the information pertains to a student and constitutes either a treatment or education record under FERPA, then the Transaction Rule will apply, but the Security and Privacy Rules will not apply.

Protection Provided: Under the Privacy Rule, use or disclosure of the protected health information is allowed only when:

1. The Privacy Rule requires or permits the disclosure, OR
2. The client or his or her representative provides written authorization.

7

SELECTED CASE STUDY

8

CASE OF NOT SETTING A CLINIC AS A HEALTHCARE COMPONENT

- Malware was installed on a workstation in the Center for Language, Speech, and Hearing

9

CASE OF NOT SETTING A CLINIC AS A HEALTHCARE COMPONENT

- OCR notified of the breach; investigation was launched on August 27, 2013
- OCR investigators discovered a number of areas of non-compliance with HIPAA Rules that directly contributed to breach

10

CASE OF NOT SETTING A CLINIC AS A HEALTHCARE COMPONENT

- Malware was a generic remote access Trojan
- Infection occurred because the Workstation was not protected by a firewall
- University ascertained that access to ePHI had been gained

11

CASE OF NOT SETTING A CLINIC AS A HEALTHCARE COMPONENT

- University was a hybrid entity and had appropriate controls in other healthcare components but did not have controls at Speech clinic
  - No risk analysis
  - No technical security measures

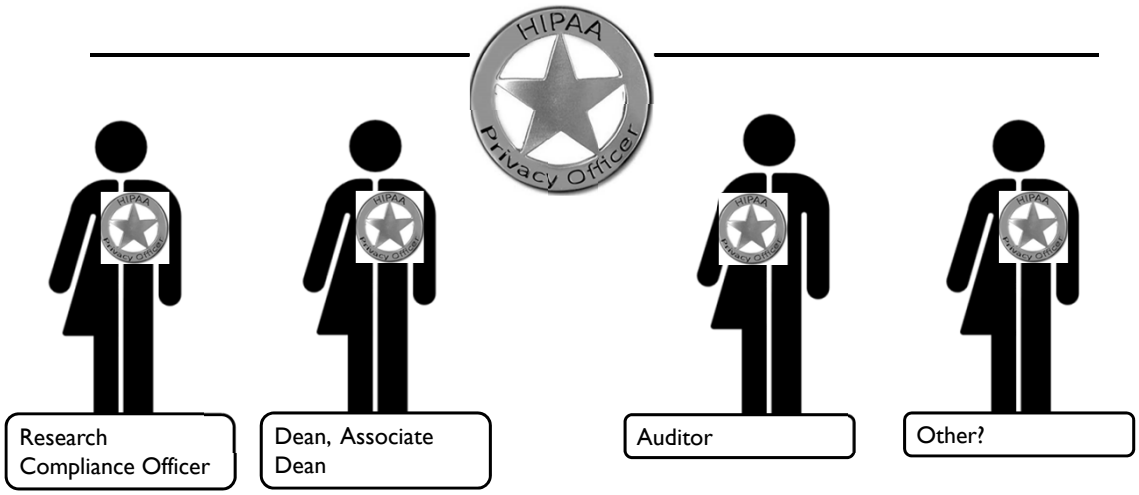
12

CASE OF NOT SETTING A CLINIC AS A HEALTHCARE COMPONENT – RESULTING ACTION ITEMS

- Enterprise-wide risk management plan to address all ePHI
- Full review of policies and procedures
- All staff take training on P&P

13

HOW MANY OF YOU HOLD OTHER TITLES?



14

PRACTICAL IMPLEMENTATION STEPS

On-Boarding IT

Training

Regular innovative communication

15

GET INFORMATION TECHNOLOGY/IT ON BOARD

- Identify and designate the HIPAA security officer within IT
  - Conduct a baseline security risk analysis
  - Standing meetings with HIPAA privacy officer and HIPAA security officer
  - Monitor University wide-data risks in the context of HIPAA
- IT advanced training led by HIPAA Security officer for IT staff

16

GET INFORMATION TECHNOLOGY/IT ON-BOARD

- Ensure Devices within the Healthcare Components are:
  - ENCRYPTED! ENCRYPTION! ENCRYPTED!
  - Tracked in University inventory system with a special designation as a HIPAA compliance device
  - Used for ePHI exclusively
    - Consider limiting BYOD for healthcare component students and staff

17

TRAINING, TRAINING, TRAINING -WORKFORCE

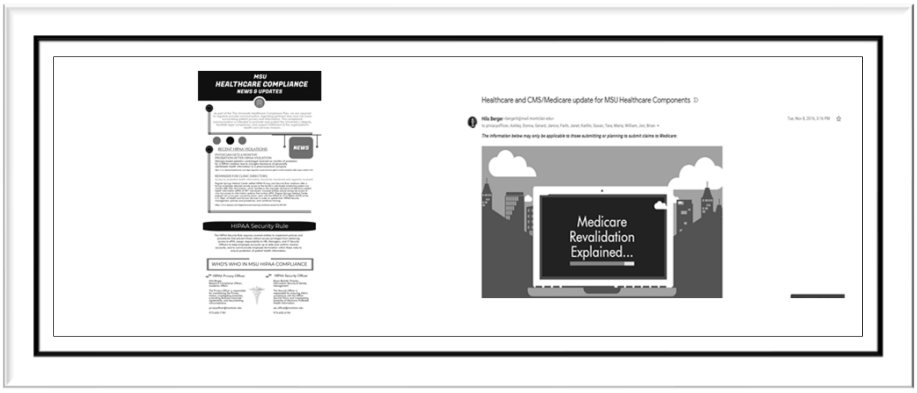
- Healthcare component staff, faculty and students can require:
- Utilizing existing training platforms rather than introducing a new one
  - CITI (HIPS course)
  - Create a quick course in Learning Management system (CANVAS, blackboard etc.)
- HIPAA Privacy Officer attending grand rounds annually for clinical groups;
  - students need this training as part of their competencies
- Privacy Officer can attend existing clinical events and ask to provide HIPAA updates

18

TRAINING/AWARENESS – BOARD OF TRUSTEES

- Connect with Chief Compliance Officer or audit team
- Link HIPAA or healthcare assessments into existing audits
- Ask for 10-15 minutes at a BOT meeting

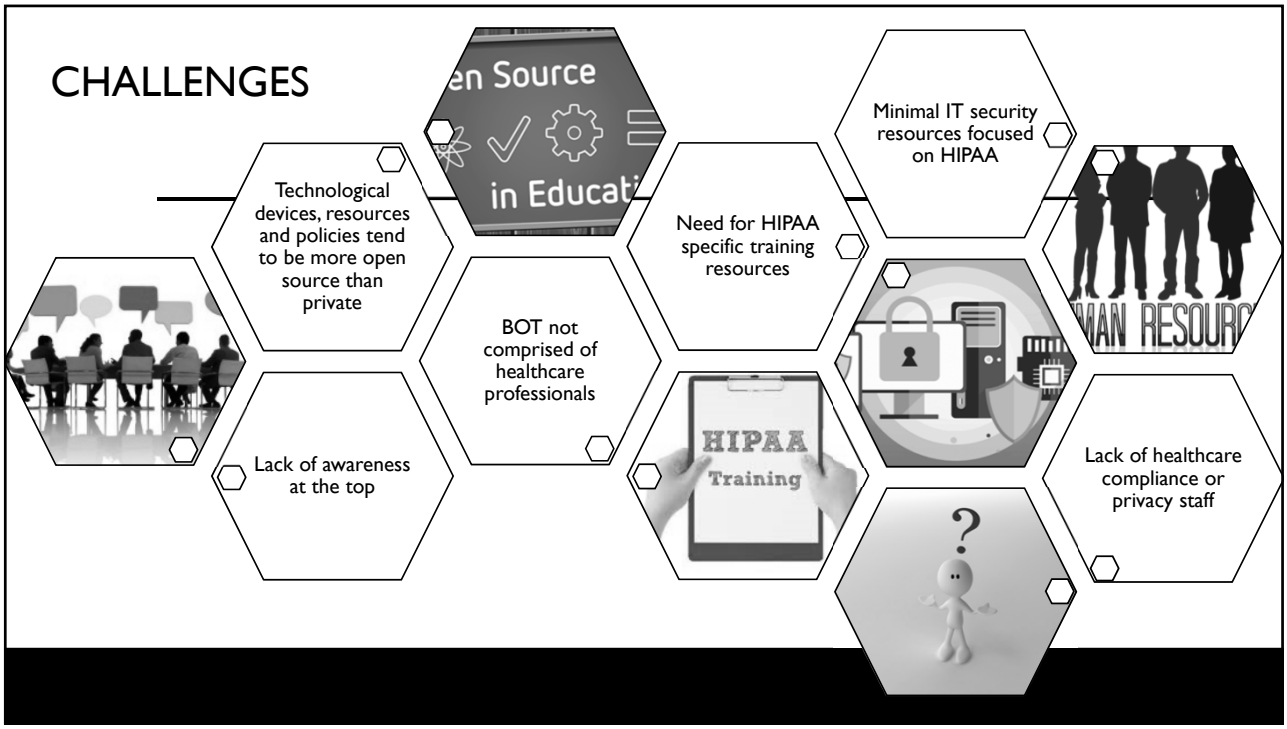
19



REGULAR COMMUNICATION PLAN

20

CHALLENGES



21

ADDITIONAL CASE STUDIES (SEE HANDOUT)

22

FINAL TAKE-AWAYS

- Learn from mistakes made by others
- Make sure you are set up as a hybrid entity and the healthcare components are taking accountability for HIPAA
- Designate your HIPAA Privacy Officer and Security Officer and provide them with practical steps for compliance
- Workforce and student training is a top priority in your healthcare components

23

THANK YOU!

Hila Berger

HIPAA Privacy Officer

Director, Research Compliance and Regulatory Programs
973-655-7781

bergerh@Montclair.edu

24

WEB REFERENCES

https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html

https://www.natlawreview.com/article/are-non-covered-activities-and-programs-your-campusinstitution-leaving-you-overly

https://datacenterfrontier.com/security-compliance-hybrid-it-strategy/

https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-what-your-staff-doesnt-know-about-hipaa-can-kill-you

https://www.hipaajournal.com/umass-to-pay-ocr-650k-to-resolve-hipaa-violations-3681/

25