Tools, Strategies & Lessons Learned to Address Unique HIPAA Issues for Universities and AMCs

MARTI ARVIN, CYNERGISTEK, INC.

KAREN PAGLIARO-MEYER, PRIVACY OFFICER, COLUMBIA UNIV. MEDICAL CENTER

TANISHA RAIFORD, COMPLIANCE & PRIVACY OFFICER, WEILL CORNELL MEDICINE

KRIS WEST, CHIEF COMPLIANCE OFFICER, EMORY UNIV.

Disclaimer:

THE VIEWS EXPRESSED IN THIS PRESENTATION BELONG TO THE SPEAKERS AND DO NOT NECESSARILY REPRESENT THE VIEWS OF THEIR ORGANIZATIONS OR OTHER ORGANIZATIONS.

NOTHING IN THIS PRESENTATION CONSTITUTES LEGAL ADVICE.

Presentation Overview

What's Your HIPAA Structure and When's the Last Time You Evaluated It?

Process for Assessing Your Privacy Program's Needs and Doing More with Less

Tools to Help Perform Privacy Program Assessments

What's Your HIPAA Structure & When's the Last Time You Evaluated it?

POLL:

Is your entity a:

A. Single Covered Entity

B. Hybrid Covered Entity

C. Covered Entity that is part of an Affiliated Covered Entity

D. No Idea – that's why I came this session

HIPAA Regulations on Hybrid Entities

Hybrid entity

- Single legal entity that is
  - A covered entity (Healthcare Provider, Health plan, Healthcare Clearinghouse)
  - With both covered and non-covered functions and
  - Designate its health care components

Covered functions

- Those functions of a covered entity the performance of which makes the entity a health plan, health care provider or health care clearinghouse.

Regulations on Hybrid Entities

Business units of the organization that engage in activities that would make them a business associate if they were a separate legal entity must be included in the health care component of the hybrid entity to the extent they engage in those BA activities.

The health care component may include a component only to the extent it performs covered functions.

What are your health care components?

Key areas of contention

- Research
- Student Health
- Self-pay health care functions
- Shared services

Defining research activities

Research

- Distinction between research involving treatment that is billable
- Research on healthy subjects with services performed within the health care component
- Is IRB/Privacy Board inside or outside the covered component?
- Committees with dual purposes
  - Radiation Safety
  - Biosafety

9

Assessing the Student Health Center

Who are its patients? Students Only?

- If students only, then data is not PHI but covered by FERPA
- Consider what happens if with students take a leave or matriculate but still have student insurance
- Staff
  - Health Center Would need to be inside the covered component if billed using standard transactions
- Student dependents
  - Health Center Would need to be inside the covered component if billed using standard transactions

What notice is required?

- FERPA for students
- HIPAA NPP for non-students
- Both?

10

Assessing Self-Pay Health Care Functions

Are there components that engage in the delivery of health care services that are only self-pay?

- Psychology clinic
- Autism assessment center
- Audiology and Speech Therapy

Will these business units be required to comply with the organization's HIPAA policies?

Assessing Shared services

Are there components that engage in the delivery of health care services that are delivered by other parties?

- Clinic within the School of Public Health but services are contracted through the faculty practice group and billed by them

Defining Other Relationships

13

POLL:

Do you know if your organization is part of one or more of the following HIPAA relationships

1. Organized Health Care Arrangement
2. Affiliated Covered Entity
3. Business Associate

Answers

A. 1 only

B. 2 only

C. 3 only

D At least two of these relationships

What type of agreements/relationships might exist?

Affiliated Covered Entity (ACE)

Organized Health Care Arrangement (OCHA)

Business Associate

15

Affiliated Covered Entity

Legal separate covered entities that are affiliated designate themselves as an ACE i.e. become a single covered entity for purposes of HIPAA

May designate the separate covered entities or any health care component of the CE

Required common ownership or control – What Does this mean? How will you demonstrate it?

Designation must be documented

What about Liability Considerations?

16

Organized Health Care Arrangement

45 CFR 160.103 -A clinically integrated care setting in which individuals typically receive health care from more than one health care provider

An organized system of health care in which more than one covered entity participates and all participating CEs

- Hold themselves out as a joint arrangement
- Participate in joint activities that include at least one of the following:
  - Utilization review
  - Quality assessments
  - Payment activities

17

Business Associates

Any component of a covered entity that is a hybrid entity must include those business functions performing BA type activities in the health care component of its hybrid entity.

- Thus no business associate agreement is required.

Entities that are part of an OHCA may be a business associate of another covered entity participating in the OCHA

18

Business Associates

Need for process to identify external BA relationships before the engagement is entered and to monitor during the engagement to assure

- The risk profile is considered
- The compliance obligations are understood
- Breach notification is properly addressed.

Lessons from the Trenches

Process for Evaluating your structure

Look at the organization chart

- Assure it is up-to-date
- Assure everyone understands the functions within the different components
- Don't assume there are not covered functions because based on the name or traditional activity of the business unit, college or school
- Don't assume the business unit engages in covered functions simply because health care services are provided

Structure Evaluation

Conduct a survey

- Assure it gives adequate descriptors and definitions for the person answering the question to provide meaningful information.
- Remind everyone that simply providing healthcare services does not make one a covered entity healthcare provider under HIPAA
- Talk to legal counsel regarding relationships with third parties and the legal relationships of the AMC.

Logistics

Don’t believe everything you read on your own website.

Membership in the covered entity may be viewed as a status symbol.

Documentation is key!

Remember to keep your materials updated as you make changes to your organization.

Think about Policy Updates and New training.

Fall Out

Process for Assessing Your Privacy Program’s Needs & Doing More with Less

POLL:

How Often DO You Assess Your Privacy Program:

A. Annually

B. Quarterly

C. Monthly

D. When There's Time

25

Process for Assessing your Program

- Effective Compliance Program Elements
  - Standards and Procedures
  - Education and Training
  - Oversight
  - Monitoring and Auditing
  - Reporting
  - Enforcement and Discipline
  - Response and Prevention

•Other Assessment Elements
- Goals / Objectives of your Privacy Program
- Challenges / Obstacles
- Culture / Risk Tolerance
- Next Review/Assessment Period

26

Poll: How do you evaluate the effectiveness of your program?

A. # of Incidents / Investigations
B. HIPAA Annual Training Pass Rate
C. # of Requests – amendment, accounting of disclosures, medical information etc.
D. # of Reportable Breach Incidents
E. Incident Trends
F. All of the Above
G. It's Complicated

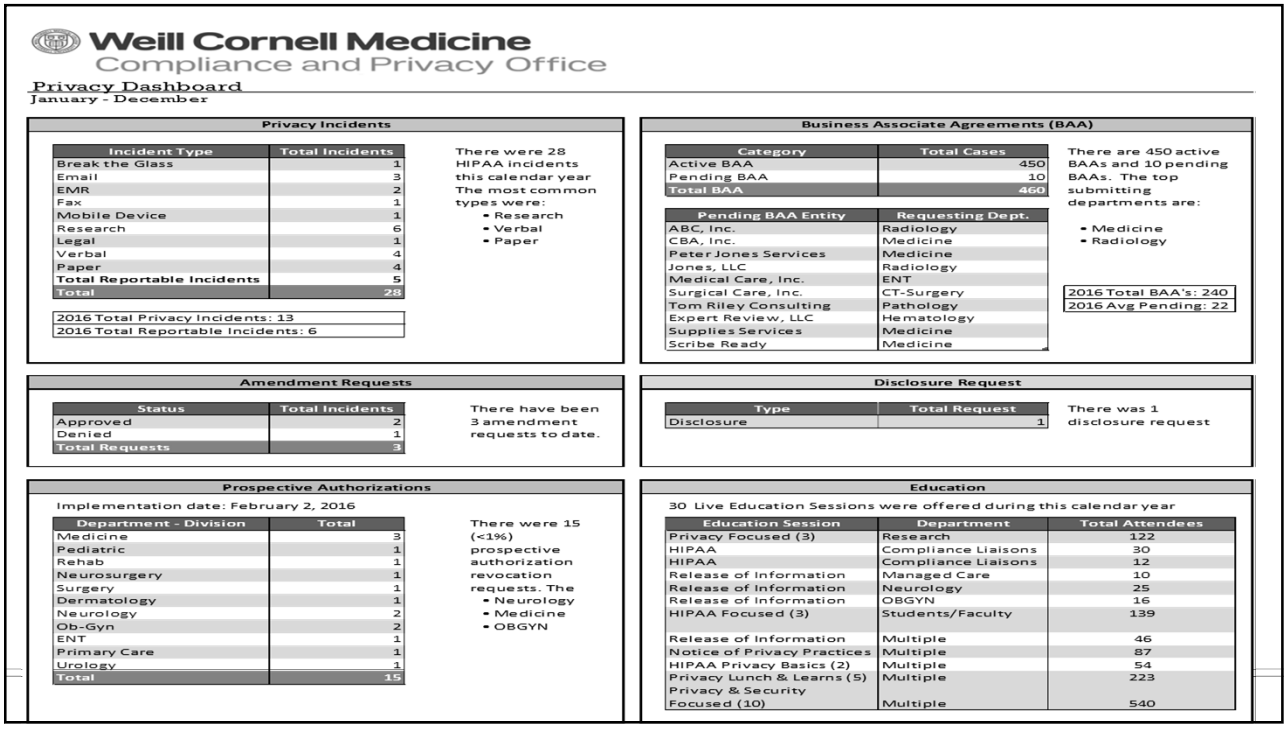
27

Doing more with less

- Policy and Procedures
- Training opportunities
- Newsletters and other communication
- Department champions – recognition
- Peer workgroups – share best practices
- Privacy role within the organization
  - Membership on other committees and workgroups
    - Human resources, quality, HIM, research

28

Tools to help perform privacy program assessments



Weill Cornell Medicine
Compliance and Privacy Office

Privacy Dashboard
January - December

Privacy Incidents

Incident Type	Total Incidents
Break the Glass	1
Email	3
EMR	2
Fax	1
Mobile Device	1
Research	6
Legal	1
Verbal	4
Paper	4
Total Reportable Incidents	5
Total	28

2016 Total Privacy Incidents: 13
2016 Total Reportable Incidents: 6

There were 28 HIPAA incidents this calendar year The most common types were:
- Research
- Verbal
- Paper

Business Associate Agreements (BAA)

Category	Total Cases
Active BAA	450
Pending BAA	10
Total BAA	460

Pending BAA Entity	Requesting Dept.
ABC, Inc.	Radiology
CBA, Inc.	Medicine
Peter Jones Services	Medicine
Jones, LLC	Radiology
Medical Care, Inc.	ENT
Surgical Care, Inc.	CT-Surgery
Tom Riley Consulting	Pathology
Expert Review, LLC	Hematology
Supplies Services	Medicine
Scribe Ready	Medicine

There are 450 active BAAs and 10 pending BAAs. The top submitting departments are:
- Medicine
- Radiology

2016 Total BAA's: 240
2016 Avg Pending: 22

Amendment Requests

Status	Total Incidents
Approved	2
Denied	1
Total Requests	3

There have been 3 amendment requests to date.

Disclosure Request

Type	Total Request
Disclosure	1

There was 1 disclosure request

Prospective Authorizations

Implementation date: February 2, 2016

Department - Division	Total
Medicine	3
Pediatric	1
Rehab	1
Neurosurgery	1
Surgery	1
Dermatology	1
Neurology	2
Ob-Gyn	2
ENT	1
Primary Care	1
Urology	1
Total	15

There were 15 (<1%) prospective authorization revocation requests. The
- Neurology
- Medicine
- OBGYN

Education

30 Live Education Sessions were offered during this calendar year

Education Session	Department	Total Attendees
Privacy Focused (3)	Research	122
HIPAA	Compliance Liaisons	30
HIPAA	Compliance Liaisons	12
Release of Information	Managed Care	10
Release of Information	Neurology	25
Release of Information	OBGYN	16
HIPAA Focused (3)	Students/Faculty	139
Release of Information	Multiple	46
Notice of Privacy Practices	Multiple	87
HIPAA Privacy Basics (2)	Multiple	54
Privacy Lunch & Learns (5)	Multiple	223
Privacy & Security Focused (10)	Multiple	540

Contact information

Marti Arvin, Cynergistek, Inc.
Marti.Arvin@cynergistek.com
512-402-8550, ext 7051

Karen Pagliaro-Meyer, Privacy Officer, Columbia Univ. Medical Center
KP155@cumc.Columbia.edu

Tanisha Raiford, Compliance & Privacy Officer, Weill Cornell Medicine
tar9009@med.cornell.org

Kris West, Chief Compliance Officer, Emory Univ.
Kwest02@emory.edu

Questions?