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

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?
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

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

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?
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

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
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

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
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

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
Tools to help perform privacy program assessments

#### Privacy Dashboard

**Weill Cornell Medicine**

**Compliance and Privacy Office**

**January - December**

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Total Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>5</td>
</tr>
<tr>
<td>Fax</td>
<td>3</td>
</tr>
<tr>
<td>Paper</td>
<td>4</td>
</tr>
<tr>
<td>Mobile Device</td>
<td>1</td>
</tr>
<tr>
<td>Research</td>
<td>6</td>
</tr>
<tr>
<td>Legal</td>
<td>1</td>
</tr>
<tr>
<td>Verbal</td>
<td>4</td>
</tr>
<tr>
<td>Total Reportable Incidents</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Total Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending BAA</td>
<td>10</td>
</tr>
<tr>
<td>Amended BAA</td>
<td>10</td>
</tr>
<tr>
<td>Finalized BAA</td>
<td>240</td>
</tr>
</tbody>
</table>

**Disclosure Request**

<table>
<thead>
<tr>
<th>Type</th>
<th>Total Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure</td>
<td>5</td>
</tr>
<tr>
<td>There was 1 disclosure request</td>
<td></td>
</tr>
</tbody>
</table>

**Prospective Authorizations**

- Medicine: 8
- Pediatric: 1
- Neurology: 1
- Surgery: 1
- Dentistry: 1
- OB/GYN: 2
- EMT: 1
- Primary Care: 1
- Overall: 15

**Implementation date: February 2, 2016**

- There were 15 implementations (25%)
- There were 5 prospective implementation requests
- The most common categories were:
  - Research
  - Legal
  - Paper

**Business Associate Agreements (BAA)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Total Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC, Inc.</td>
<td>10</td>
</tr>
<tr>
<td>LabCorp</td>
<td>10</td>
</tr>
<tr>
<td>Medical Care, Inc.</td>
<td>1</td>
</tr>
<tr>
<td>Rush University</td>
<td>2</td>
</tr>
<tr>
<td>Expert Review, LLC</td>
<td>3</td>
</tr>
<tr>
<td>Surgery Clinic</td>
<td>1</td>
</tr>
<tr>
<td>Radiology</td>
<td>2</td>
</tr>
<tr>
<td>Surgery Dept.</td>
<td>1</td>
</tr>
<tr>
<td>Anesthesiology</td>
<td>1</td>
</tr>
<tr>
<td>Cardiology</td>
<td>1</td>
</tr>
<tr>
<td>Hematology</td>
<td>1</td>
</tr>
<tr>
<td>Orthopedics</td>
<td>1</td>
</tr>
<tr>
<td>OBGYN</td>
<td>1</td>
</tr>
<tr>
<td>Urology</td>
<td>1</td>
</tr>
<tr>
<td>Overall: 41</td>
<td></td>
</tr>
</tbody>
</table>

**Disclosure Request**

<table>
<thead>
<tr>
<th>BAA Type</th>
<th>Total Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>There was 1 disclosure request</td>
<td></td>
</tr>
</tbody>
</table>

**Education**

- 80 live education sessions were offered during this calendar year
  
<table>
<thead>
<tr>
<th>Education Session</th>
<th>Department</th>
<th>Total Mine</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Focused</td>
<td>Research</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>Compliance</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>Medicine</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Release of Information</td>
<td>Neurology</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Release of Information</td>
<td>OB/GYN</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>HIPAA Focused</td>
<td>Students/Faculty</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>Release of Information</td>
<td>Multiple</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>Notice of Privacy Rights</td>
<td>Multiple</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>HIPAA Privacy Briefs</td>
<td>Multiple</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Privacy’s dashboards</td>
<td>Multiple</td>
<td>223</td>
<td></td>
</tr>
<tr>
<td>Forensics</td>
<td>Multiple</td>
<td>540</td>
<td></td>
</tr>
</tbody>
</table>

*The submission departments are: Medicine, Radiology, Surgery Clinic, Cardiology, Orthopedics, Anesthesiology, and Urology.*
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?