HIPAA Compliance in Community Partnerships

#TRCCWebSeries

Michelle Berger Marshall  
Managing Director  
Community Health & Nutrition  
Feeding America

Sarah Downer  
Clinical Instructor  
CHLPI

Katie Garfield  
Staff Attorney  
CHLPI
HOW HIPAA AFFECTS YOUR HEALTH CARE PARTNERSHIP

MAY 23, 2017
Food Banks As Partners in Health Promotion: Concerns about HIPAA and Patient Privacy

Michelle Berger Marshall
Managing Director, Community Health & Nutrition
The Need for HIPAA Guidance

- Food Banks and CBOs work with health partners to address food insecurity

- **Screen for food insecurity & intervene through referrals** to programs to access to healthy food

- Partners may want to be able to share PHI

- **Our Goal:** Understand how to build effective partnerships and ensure we comply with HIPAA regulations

- [http://tinyurl.com/FAHIPAA](http://tinyurl.com/FAHIPAA)
Connecting People to Healthy Food

Screen Patients for Food insecurity using the Hunger Vital Sign™ 2-question screener, then:

- Provide healthy **food boxes** or meal to patients at clinics or hospitals
- Food bank brings **mobile** produce distribution to the outpatient clinic
- Create **on-site pantries** in outpatient clinics
- Refer patients to local **food pantries**
- Support for **SNAP** applications or other benefits
Training center for the next generation of health and food lawyers, law and policy reform think tank, advocacy leadership development and law reform advising program.

**Health Law**
- Access to health care for low-income populations
- Preventive health care & chronic disease management

**Social Determinants of Health Interventions**

**Food Law**
- Access to healthy food
- Sustainable food systems
WHAT IS HIPAA?

- **Health Insurance Portability and Accountability Act of 1996**
- Implementing Regulations
  - Privacy Rule
  - Security Rule (e-PHI)
  - Enforcement Rule
  - Omnibus Rule
  - Breach Notification Rule
- Enforced by the U.S. Department of Health and Human Services (HHS)
**Why Is HIPAA Important for CBOs?**

1. HIPAA is extremely important to potential health care partners.

2. It is important for Community-Based Organizations (CBOs) to understand the basic tenets of HIPAA in order to be good self-advocates as they form new partnerships.

3. As CBOs work with health care partners and expand the services they provide, some of their activities might resemble the provision of health care.
**WHAT INFORMATION DOES HIPAA COVER?**

- Individually Identifiable Health Information
  = Protected Health Information (PHI)

- PHI can include
  - Name
  - Birthday
  - Phone Number
  - Address
  - SSN
  - Diagnosis/Condition
  - Blood Pressure
WHO MUST COMPLY WITH HIPAA?

- **Covered Entities (CEs)**
  1. Health Plans
  2. Health Care Clearinghouses (Data Conversion)
  3. Health Care Providers that transmit PHI electronically for certain specified transactions (including sending insurance claims)

- **Business Associates (BAs)**
  1. Provide legal, actuarial, consulting, data aggregation, management, administrative, financial, or accreditation services to a CE
  2. Conduct activities on behalf of a CE
A Covered Entity health provider can share information about patients with food banks if they adopt a patient-driven method of sharing PHI.

- The Covered Entity obtains the patient’s request or authorization to disclose certain information or allows the patient to be the disclosing party

- Allows collaboration without requiring CBOs to assume extra responsibilities/liability under HIPAA
  - Does not require a Business Associate Agreement (BAA)
  - Would not, on its own, make a CBO covered by HIPAA
Example Scenario: The patient completes a written request or authorization form for the provider to share PHI with the food bank.

1. The patient completes the request or authorization form
2. The health care provider sends the food bank the patient’s contact details and pertinent health information
3. The food bank conducts outreach to the patient and prepares the food box
Who Must Comply with HIPAA?

- **Covered Entities (CEs)**
  1. Health Plans
  2. Health Care Clearinghouses (Data Conversion)
  3. Health Care Providers that transmit PHI electronically for certain specified transactions (including sending insurance claims)

- **Business Associates (BAs)**
  1. Provide legal, actuarial, consulting, data aggregation, management, administrative, financial, or accreditation services to a CE
  2. Conduct activities on behalf of a CE
As a Business Associate

Providing specific services to a Covered Entity

- Legal, actuarial, consulting, data aggregation, management, administrative, financial, or accreditation services
- Generally not CBOs

Conducting activities “on behalf of” a Covered Entity

OR:

- Assisting Covered Entities with “health care operations”
- Health care operations include population-based activities to improve patient health
Health care partners may prefer to have CBOs sign BAAs

- A BAA allows the partner to share patient information without a patient’s authorization or written request
- The health care partner may be accustomed to signing BAAs with external organizations

A BAA is a contract that would require a CBO to incur legal responsibilities and liability for handling PHI
**Before Signing a BAA:**

- Ask your partner if your goals could be met using a patient-driven model for sharing PHI.
- Read the BAA. If you do **not** understand the provisions, request clarification.
- Conduct a realistic assessment of whether you can meet the responsibilities/obligations in the contract. If not, do **not** sign the BAA. Look for different ways to partner.
- Consult an attorney. Look for pro bono legal help when cost is a factor.
WHO MUST COMPLY WITH HIPAA?

- **Covered Entities (CEs)**
  1. Health Plans
  2. Health Care Clearinghouses (Data Conversion)
  3. Health Care Providers that transmit PHI electronically for certain specified transactions (including sending insurance claims)

- **Business Associates (BAs)**
  1. Provide legal, actuarial, consulting, data aggregation, management, administrative, financial, or accreditation services to a CE
  2. Conduct activities on behalf of a CE
As a Covered Entity – Health Care Provider

1. Providing “medical or health services” or “health care”

2. Transmitting health information electronically in connection with a covered transaction
The HIPAA rules include references to illustrative examples of “medical or health services.” These examples include:

- Diabetes outpatient self-management training services

As CBOs expand their services, they may come closer to providing “medical or health services” and therefore be considered health care providers.

- If CBOs also transmit health information electronically for covered transactions such as billing, they could qualify as CEs.

When Else Might HIPAA Apply to CBOs?

- The HIPAA rules define “health care” as follows:
  - Health care means care, services, or supplies related to the health of an individual. Health care **includes, but is not limited to**, the following:
    (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
    (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

- CBOs that use medical terms such as “prescription” when describing their services may also be considered health care providers.

Source: 45 C.F.R. § 160.103 (emphasis added).
WHAT DOES IT MEAN TO COMPLY WITH HIPAA?

CEs and BAs must take steps to keep PHI secure while providing patients access to their own PHI

- Be prepared to invest time and resources to:
  - **Assess Risk**: Develop a Security Management Plan to identify risks, vulnerabilities, mitigation strategies
  - **Develop and Document Policies**: Document policies/procedures adopted to protect PHI
  - **Train Staff**: Develop and implement training materials to inform all workforce members about HIPAA and relevant HIPAA-related policies
  - **Invest in Physical Safeguards and Technology to Protect PHI**: Invest in equipment, technology, software, locks, and other physical measures to protect PHI
Step 1: Conduct a Risk Analysis

▪ Designate a Security Officer

▪ Preview Security Risk:
  – Use resources such as ONC’s Security Risk Assessment Tool

▪ Review Existing Policies to Protect PHI:
  – Where does PHI exist?
  – What potential threats/vulnerabilities exist? How serious are such threats?

▪ Document Your Process, Findings, and Actions
Step 2: Develop an Action Plan to Protect PHI and Mitigate Risk

- Convene a team

- Decide which strategies to use
  - Which strategies are realistic and effective?

- Develop the Action Plan
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
  - Organizational Standards
  - Policies and Procedures

Adapted from the federal Office of the National Coordinator for Health Information Technology’s (ONC’s) “Sample Seven-Step Approach for Implementing a Security Management Process”
### Developing a Security Management Plan

<table>
<thead>
<tr>
<th>Security Component</th>
<th>Examples of Vulnerabilities</th>
<th>Examples of Security Mitigation Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrative Safeguards:</strong></td>
<td>• No security officer is designated.</td>
<td>• Security officer is designated and publicized.</td>
</tr>
<tr>
<td>• designed to manage the selection, development, implementation, and maintenance of security measures</td>
<td>• Workforce training begins at hire and is conducted regularly and frequently.</td>
<td>• Workforce training begins at hire and is conducted regularly and frequently.</td>
</tr>
<tr>
<td>• should protect electronic PHI</td>
<td>• Periodic security assessment not done.</td>
<td>• Security risk analysis is performed periodically and when a change occurs in the practice or technology.</td>
</tr>
<tr>
<td>• should manage the conduct of the covered entity’s workforce in relation to the protection of that information</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical Safeguards:</strong></td>
<td>• Facility has insufficient locks and other barriers to protect data access.</td>
<td>• Building alarm systems are installed.</td>
</tr>
<tr>
<td>• designed to protect electronic PHI as well as buildings and equipment</td>
<td>• Computer equipment is easily accessible by the public.</td>
<td>• Offices are locked.</td>
</tr>
<tr>
<td>• should address natural and environmental hazards and unauthorized intrusion</td>
<td>• Portable devices are not tracked or not locked up when not in use.</td>
<td>• Screens are shielded from secondary viewers.</td>
</tr>
<tr>
<td><strong>Technical Safeguards:</strong></td>
<td>• Audit logs are not used enough to monitor users and activities.</td>
<td>• Secure user IDs, passwords, and appropriate role-based access are used.</td>
</tr>
<tr>
<td>• designed to address technology and related policies and procedures</td>
<td>• No measures are in place to keep electronic patient data from improper changes.</td>
<td>• Routine audits of access and changes to technology are conducted.</td>
</tr>
<tr>
<td>• should protect electronic PHI and control access to it</td>
<td>• No contingency plans exist.</td>
<td>• Anti-hacking and anti-malware software is installed.</td>
</tr>
<tr>
<td><strong>Organizational Standards:</strong></td>
<td>• Electronic exchanges of patient information are not encrypted or otherwise secured.</td>
<td>• Contingency plans and data backup plans are in place.</td>
</tr>
<tr>
<td>• designed to address requirements related to contracts with other organizations (e.g., covered entity, subcontractor)</td>
<td></td>
<td>• Data is encrypted.</td>
</tr>
<tr>
<td><strong>Policies and Procedures:</strong></td>
<td>• No breach notification and associated policies exist.</td>
<td>• Regular reviews of agreements are conducted and updates made accordingly.</td>
</tr>
<tr>
<td>• designed to identify and implement reasonable and appropriate policies and procedures for HIPAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Generic written policies and procedures to ensure HIPAA security compliance were obtained but not tailored to the organization or followed by the organization.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• The manager performs ad hoc security measures.</td>
<td>• Written policies are procedures are implemented and staff is trained.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Security team conducts monthly review of user activities.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Routine updates are made to document security measures.</td>
<td></td>
</tr>
</tbody>
</table>

Developing A Security Management Plan

Step 3: Implement Action Plan to Protect PHI

▪ Implement the Action Plan

▪ Prevent Breaches by Educating and Training Your Workforce
  – Train your ENTIRE workforce every year or in the event of changes to your polices/procedures.

▪ Periodically Update Your BAAs

Adapted from the federal Office of the National Coordinator for Health Information Technology’s (ONC’s) “Sample Seven-Step Approach for Implementing a Security Management Process”
Step 4: Periodically Review/Update Risk Mitigation Plan

- Monitor, Audit, and Update Security Strategies on an Ongoing Basis
  - Are audit controls in place?
  - Are you able to conduct an audit?

Adapted from the federal Office of the National Coordinator for Health Information Technology’s (ONC’s) “Sample Seven-Step Approach for Implementing a Security Management Process”
Key Takeaways

- HIPAA regulates the use of Protected Health Information (PHI) by Covered Entities (CEs) and their Business Associates (BAs).
- In most cases, CBOs are not CEs or BAs.
- CBOs that are not BAs do not need to sign Business Associate Agreements (BAAs).
- Instead of signing BAAs, Covered Entities can obtain patient requests or authorizations to share information with CBOs.
- If CBOs decide to become CEs or BAs, they should be prepared to devote resources to becoming HIPAA-compliant.
Next Steps

- Bring together stakeholders to highlight issues in applying HIPAA to CBOs
  - When do CBOs cross the line to become CEs/BAs?
  - Did legislators/regulators intend that impact?

- Seek formal guidance to clarify application to CBOs and ensure that HIPAA does not become a barrier to innovative partnerships
QUESTIONS?

Sarah Downer
sdowner@law.harvard.edu

Katie Garfield
kgarfield@law.harvard.edu
Questions?