





Food Banks as Partners in Health Promotion:

How HIPAA and Concerns about Protecting Patient Information Affect Your Partnership

March 2017

CHLPI CENTER for HEALTH LAW and POLICY INNOVATION
HARVARD LAW SCHOOL

FEEDING AMERICA

TABLE OF CONTENTS

ABOUT THE AUTHORS....i

FOOD BANKS AS PARTNERS IN HEALTH PROMOTION: AN OVERVIEW....1

EXECUTIVE SUMMARY....3

WHAT IS HIPAA?....5

- What Entities Must Comply with HIPAA?....5

WHY DO FOOD BANKS NEED TO KNOW ABOUT HIPAA?....5

PATIENT-DRIVEN INFORMATION SHARING BETWEEN FOOD BANKS AND COVERED ENTITIES....7

- Written Disclosure Requests....7
- Valid Authorizations to Disclose PHI....7
- Navigating HIPAA When Sharing Information with Health Care Partners: Examples....7

WHEN MIGHT A FOOD BANK BE SUBJECT TO HIPAA REQUIREMENTS?....10

- Food Banks as Health Care Providers/Covered Entities?....10
- Food Banks as Business Associates?....14
- Business Associate Agreements: What They Are and What They Mean....14

WHAT IT MEANS TO COMPLY WITH HIPAA....17

- Four Steps to Developing a Security Management Plan for Business Associates....17
  - STEP 1: Conduct a Risk Analysis....17
  - STEP 2: Develop an Action Plan to Protect PHI and Mitigate Risk....18
  - STEP 3: Implement Action Plan to Protect PHI....21
  - STEP 4: Review and Update the Risk Mitigation Action Plan Periodically....21

CONCLUSION....22

APPENDIX I: Patient's Written Authorization to Disclose Health Information....23

APPENDIX II: Business Associate Agreement....25

APPENDIX III....29

- Requirements under the HIPAA Security Rule for Covered Entities and Business Associates....29
- Requirements under Breach Notification Rule for Covered Entities and Business Associates....30
- Requirements for Business Associates under Privacy Rule....31

ABOUT THE AUTHORS

CHLPI

The Center for Health Law and Policy Innovation of Harvard Law School (CHLPI) advocates for legal, regulatory, and policy reforms to improve the health of underserved populations, with a focus on the needs of low-income people living with chronic illnesses. CHLPI works with consumers, advocates, community-based organizations, health and social services professionals, food providers and producers, government officials, and others to expand access to high-quality health care and nutritious, affordable food; to reduce health disparities; to develop community advocacy capacity; and to promote more equitable and effective health care and food systems. CHLPI is a clinical teaching program of Harvard Law School and mentors students to become skilled, innovative, and thoughtful practitioners as well as leaders in health, public health, and food law and policy.

This resource is the second in a series that highlights opportunities and considerations for food banks that want to work more closely with the health care system to better serve clients and patients. The first publication in this series, *Food Banks as Partners in Health Promotion: Creating Connections for Client and Community Health*, was released in 2015 and is available at www.chlpi.org.

Feeding America

Feeding America is a nationwide network of 200 member food banks that serve all 50 states, the District of Columbia, and Puerto Rico. As the largest domestic hunger-relief charity in the United States, the Feeding America network of food banks provides food assistance to an estimated 46.5 million Americans in need each year, including 12 million children and 7 million seniors. The Feeding America national office supports member food banks across the country by securing food and funds for the local food banks; by building partnerships that benefit the network nationally and also provide support for food bank programs; by supporting programs that help improve food security among the people and communities we serve; and by raising awareness about the problem of hunger and advocating on behalf of food-insecure Americans. In turn, food banks distribute food and groceries to 60,000 food pantries and meal programs that directly serve people in need across the U.S.

Food Banks as Partners in Health Promotion: How HIPAA and Concerns about Protecting Patient Information Affect Your Partnership is written by Gideon Palte, Dalia Deak, Sarah Downer, Katie Garfield, and Kim Prendergast.

The Center for Health Law and Policy Innovation provides information and technical assistance on issues related to health reform, public health, and food law. It does not provide legal representation or advice. This document should not be considered legal advice. For specific legal questions, consult an attorney.

FOOD BANKS AS PARTNERS IN HEALTH PROMOTION: AN OVERVIEW

Food banks and food pantries[1] are a critical part of the response to food insecurity and hunger in the United States. They also have a role to play in supporting the health of people who are food insecure and who have, or are at risk for, certain health conditions.

Food insecurity is the lack of sufficient food to live an active, healthy life.[i]

Food insecurity has a negative impact on health outcomes and interferes with management of illness or other health concerns that are common among food bank clients.[2] In 2014, 47% of food bank clients reported "fair" or "poor" health.[3] In the same year, 33% of food bank client households reported having at least one member with diabetes, and 58% reported having at least one member with hypertension.[4]

Nutrition affects the onset, management, and outcome of many health conditions, including but not limited to: [ii]

- Diabetes
- Kidney Disease
- Certain Cancers
- HIV
- Stroke
- Heart Disease
- Obesity

Food banks can work with local health care providers (e.g. doctors, nurses, and hospitals) and health care payers (e.g., health insurers, including private health insurance companies, Medicaid, and Medicare) to ensure that clients and patients with health concerns have access to healthy, nutritious foods.

Health care providers and payers are increasingly looking outside of the clinical setting at factors that impact the health of their patients. These factors—which include economic stability, education, social and community environment, safe and affordable housing, immigration status, public safety, and availability of healthy foods—are called social determinants of health.[5] New payment models for health care services seek to reward better clinical outcomes for patients, giving health care providers a financial incentive to find new approaches to address social determinants of health in their patient populations.[6]

Social determinants of health are the conditions in the places where people live, work, and learn that affect their overall health. According to the Centers for Disease Control and Prevention, these conditions include economic stability, education, social and community environment, safe and affordable housing, public safety, and availability of healthy foods.[iii]

Food insecurity is a key social determinant of health. Children in households that are food insecure fall ill more frequently, are hospitalized more often, and take longer to recover after getting sick.[7] Individuals who are food insecure are also twice as likely to have type 2 diabetes.[8] Due to these and other effects of food insecurity on health, the American Academy for Pediatrics and the American Diabetes Association, among others, have recommended that health care providers screen for food insecurity in clinical care settings.[9] Increased screening for food insecurity means increased awareness among providers about the challenges their patients face in accessing food.

The American Academy of Pediatrics, Children's Health Watch, and others recommend that health care providers ask patients the following two questions in order to screen for food insecurity:

1. **Within the past 12 mo, we worried whether our food would run out before we got money to buy more. Was that often, sometimes, or never true?**
2. **Within the past 12 mo, the food we bought just didn't last and we didn't have money to get more. Was that often, sometimes, or never true?**

An answer to either question of often true or sometimes true indicates food insecurity.[iv]

Health care providers and payers are increasingly seeking to collaborate with food banks to ensure that food insecure patients receive nutrition assistance. Active partnerships between food banks and health care providers have tangible benefits for patients. Research shows that proactive outreach from a community food resource provider that receives a food insecure patient's name and contact information is significantly more likely to result in the patient receiving food assistance.[10] However, these collaborations between food banks and health care providers often require

communication about the needs of patients and clients. With more communication between food banks and the health care system comes increased responsibility to think critically about how information that relates to patients and clients is shared and protected.

Health care providers are legally required to keep patient information private and secure. This legal obligation has been embodied in federal law through the Health Insurance Portability and Accountability Act of 1996[11] and its implementing regulations[12] (referred to collectively as "HIPAA" in this resource).

The federal law that governs the way health care entities use and protect information about patients is the Health Insurance Portability and Accountability Act of 1996 (known as HIPAA).[v]

HIPAA seeks to encourage the exchange of patient information in order to improve care while ensuring that this information remains protected and private.[13] While food banks have always been aware of the need to respect the privacy and dignity of their clients by handling client information carefully, there is no equivalent law to HIPAA that governs how food banks must handle client information. Most health care payers and providers, by contrast, have an obligation under HIPAA to protect health information that can be used to individually identify a patient. Potential health care partners will therefore want to know that food banks have considered how they can keep the information that might be shared with them private and secure. Moreover, in some cases, health care providers will ask food bank partners to sign a contract to become a Business Associate, thereby obligating food banks themselves to comply with many HIPAA requirements. This resource will provide an overview of how HIPAA influences information-sharing between health care providers and food banks and provide strategies for effective coordination and communication to keep health information safe.





EXECUTIVE SUMMARY

This resource is written to and for food bank staff in order to help them understand how HIPAA affects potential partnerships with health care providers and other "Covered Entities" under HIPAA. HIPAA is a set of federal laws and regulations that protect health information that can be used to individually identify a patient.[14] This information is referred to as Protected Health Information (PHI) under HIPAA.[15]

Examples of individually identifiable health information, which becomes protected health information (PHI) under HIPAA when held by a Covered Entity or Business Associate, include: [vi]

- **Name**
- **Address**
- **Birth date**
- **Social security number**
- **Information relating to an individual's physical or mental health condition**

HIPAA applies to certain Covered Entity health care individuals and organizations, as well as their Business Associates.[16] Covered Entities under HIPAA include health plans, health care clearinghouses (which convert patient information into a standard format for billing), and health care providers that transmit health information electronically for certain specified purposes.[17] Business Associates are individuals or organizations that are separate from Covered Entities but that require access to PHI in order to provide certain services to or on behalf of Covered Entities.[18]

HIPAA applies to: Covered Entities and their Business Associates. Covered Entities are health plans, health care clearinghouses, and health care providers that transmit patient data electronically for certain specified purposes. Business Associates are individuals or organizations that use protected health information (PHI) to provide certain services to Covered Entities.[vii]

In order for food banks to avoid taking on new responsibilities when it comes to handling client information, food banks and their Covered Entity health care partners can adopt a patient-driven method of sharing information. Under HIPAA rules, a Covered Entity can disclose a patient's health information to a food bank by obtaining a written request or authorization from the patient to do so.[19] Covered Entities may use standard disclosure request or authorization forms that patients complete in order to request or authorize disclosure of their health information to a food bank.[20] Using patient requests or authorizations is a straightforward way for food banks and their health care partners to collaborate in a manner that is consistent with HIPAA requirements and that does not require the food bank to assume legal liability under HIPAA.

Covered Entities can have patients complete standard disclosure request or authorization forms to share information with food banks and food pantries. Food banks and food pantries can also distribute written disclosure request forms to their clients to bring to their next medical appointment.[viii]

Typically, HIPAA does not apply to food banks because food banks do not conduct activities that would make them organizations covered by HIPAA. However, in some circumstances, food banks could become regulated by HIPAA if they provide and bill for health care or perform services on behalf of HIPAA-regulated entities. For example, if food banks provide and electronically bill for Medical Nutrition Therapy, they could become Covered Entity health care providers. If food banks perform health care operations on behalf of a Covered Entity, they may become Business Associates.[21] As either a Covered Entity or a Business Associate, a food bank would have a legal obligation to comply with HIPAA requirements.[22] For more details on what complying with HIPAA requires, refer to *What It Means to Comply with HIPAA* on p. 17.

In most cases, food banks are NOT Covered Entities or Business Associates under HIPAA and therefore have no obligation to comply with HIPAA requirements.

Even if a food bank does not meet the definition of Business Associate, potential health care partners may want to treat it as one because doing so would allow the Covered Entity to share patient information without a patient's authorization or written request. Moreover, many Covered Entities may be accustomed to forming Business Associate partnerships.

Becoming a health care Covered Entity's Business Associate means the food bank must sign a Business Associate Agreement with the Covered Entity.[23] Food banks should exercise caution before agreeing to become Business Associates, a designation which comes with obligations to comply with HIPAA requirements.[24] For more details on what a Business Associate Agreement entails, refer to *Business Associate Agreements: What They Are and What They Mean* on p. 14, as well as to the *Business Associate Agreement Template* provided in Appendix II.

This resource will provide examples of how food banks can work with health care entities within the boundaries of HIPAA to receive information about patients who are food insecure. Each food bank and food bank/health care partnership is unique. The information presented here is not legal advice and does not replace the role of an attorney in providing advice about a specific food bank/health care partnership. It does not cover applicable state laws and regulations that add to or differ from responsibilities bestowed by HIPAA.[25] For additional information about HIPAA, refer to the following webpage maintained by the United States Department of Health and Human Services (HHS): http://www.hhs.gov/hipaa/for-professionals/index.html. If you are ever unsure about how HIPAA applies to your food bank or how to best construct a partnership with a health care partner, consult an attorney.[26] If cost of legal services is a factor, law firms may be able to provide legal services at no cost through a pro bono program.





WHAT IS HIPAA?

In the mid-1990s, with the increasing flow of health information across state lines among health care providers, hospitals, and insurers, the federal government sought to standardize the privacy protections for health information in the United States.[27] The need for such protections became even more apparent with the increasing use of technology in health care and the electronic storage of health information.[28] In 1996, Congress responded to these new developments by passing a law known as HIPAA.[29]

HIPAA stands for the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996.[30] This law required the federal government to adopt privacy protections for health information that can be used to identify an individual and that is held by certain types of organizations, called "Covered Entities."[31] Since 1996, the federal government has taken numerous actions in order to implement HIPAA and further its purpose of protecting health information.

When this resource mentions rights or obligations under HIPAA, it refers to the requirements and provisions found in all of the laws and regulations below.

2000 — **2017**

Between 2000 and 2006, the United States Department of Health and Human Services (HHS), the federal agency charged with implementing HIPAA, issued the **Privacy Rule**, the **Security Rule**, and the **Enforcement Rule** in order to give effect to the Act's privacy protections for patient information held by Covered Entities.[32]

In 2009, Congress passed the **Health Information Technology for Economic and Clinical Health (HITECH) Act**, which amended some provisions of HIPAA that relate to the storage and transmission of electronic protected health information (e-PHI) and which gave HHS the authority to make Business Associates of Covered Entities directly liable under HIPAA rules.[33]

HHS subsequently amended the **Enforcement Rule** and issued the Omnibus Rule pursuant to the HITECH Act.[34] The **Omnibus Rule** also finalized the Breach **Notification Rule**, which specifies required notifications for breaches of PHI.[35]

WHAT ENTITIES MUST COMPLY WITH HIPAA?

HIPAA protects health information that can be used to identify someone individually and pertains to **Covered Entities** and their **Business Associates**.[36] **Covered Entities** under HIPAA are:

1) health plans,
2) health care clearinghouses (which convert health data for billing purposes), and
3) health care providers that transmit information electronically for certain specified purposes.[37]

Business Associates are individuals or organizations that are separate from Covered Entities but that require access to protected health information (PHI) in order to provide certain services to or on behalf of Covered Entities.[38]



WHY DO FOOD BANKS NEED TO KNOW ABOUT HIPAA?

It's important for food banks to have basic familiarity with HIPAA for three reasons.

(1) Food banks should be familiar with HIPAA because HIPAA is extremely important to their health care partners and collaborators. While the core activities of food banks are not regulated by HIPAA, health care partners and collaborators are subject to a set of laws and regulations that govern how they use and share patient information. These requirements can be complicated to navigate and failing to comply with them can have significant negative consequences. Food banks' ability to properly handle patient information will encourage more health care providers and payers to become their partners.

(2) As food banks start to work with health care partners and expand the services that they provide to clients, the new activities they perform might resemble the provision of health care. If food bank activities come too close to this line, the food bank itself could meet the definition of an entity that would be required to comply with HIPAA, thus adding significant responsibilities to handling client information.

(3) Finally, it is important for food banks to understand the basic tenets of HIPAA in order to be good self-advocates as they form new partnerships. Becoming a Business Associate of a health care Covered Entity requires significant investment in assessing the security of information that could be considered PHI, training staff on how to handle such information, and developing numerous policies and procedures that describe how a food bank is maintaining and protecting such information. Being realistic about the new tasks and responsibilities that they will incur in the course of partnership will help food banks and their health care partners find creative ways to serve patients and clients in ways that best address food insecurity and health without creating unnecessary burdens or over-stating the capacity to receive, store, and guard sensitive patient information. It will also help food banks take active steps over time to institute information-holding and sharing methods that are HIPAA-compliant.





PATIENT-DRIVEN INFORMATION SHARING BETWEEN FOOD BANKS AND COVERED ENTITIES

Patient-driven methods of information disclosure are consistent with HIPAA requirements. When a patient makes a **disclosure request** or completes a valid **written authorization** for a Covered Entity to share information with a food bank, the Covered Entity does not need any type of agreement with the food bank in order to share the patient's information.[39] Having patients complete written disclosure requests or authorizations is a straightforward way for Covered Entities to share patient information with food banks in a manner consistent with HIPAA requirements.

Having patients complete written disclosure request or authorization forms is likely the most straightforward way for Covered Entity health care providers to share patient information with food banks and food pantries in a manner consistent with HIPAA requirements.

To obtain patient authorization or written permission to disclose PHI, Covered Entities can have patients complete forms when they:

- Check in for a visit;
- Meet with the doctor or another provider; or
- Make their next appointment or receive a visit summary after the visit is complete.

Food banks can:

- Give clients a form to complete and present to the doctor or provider during the client's next health care visit; or
- Have clients complete an authorization form that food bank staff can fax to the health care provider.

WRITTEN DISCLOSURE REQUESTS

Food banks and Covered Entities can help patients request that their health information be disclosed to food banks. Subject to limited exceptions, patients have a right to access their health information held by Covered Entities.[40] This right of access includes the right to direct the Covered Entity to send the information to a recipient of the patient's choosing.[41] The Covered Entity must comply with such a request that (1) is written, (2) is signed by the patient, and (3) clearly identifies the intended recipient.[42] Generally, the Covered Entity must act on the request within thirty days.[43]

Under most circumstances, a Covered Entity must comply with such a request that

(1) is **written**,

(2) is **signed by the patient**, and

(3) **clearly identifies the intended recipient**.[ix]

VALID AUTHORIZATIONS TO DISCLOSE PHI

Covered Entities may share PHI when there is a valid written disclosure authorization from the patient.[44] A written authorization to share PHI would permit the Covered Entity to send the patient's information to the food bank but, unlike written requests, would not create an obligation for it to do so.[45]

You will find a sample authorization form in Appendix I.

NAVIGATING HIPAA WHEN SHARING INFORMATION WITH HEALTH CARE PARTNERS: EXAMPLES

When working with health care partners, it is important to understand both what information HIPAA protects and to which organizations HIPAA applies. HIPAA protects only individually identifiable information that is created, used, or maintained by an organization subject to HIPAA requirements.[46] **Remember that the patient can always voluntarily disclose any or all of her health information.**

Refer to the table below for some examples of ways that you can partner with health care providers and payers, share information, and better meet the health-related needs of your clients.

Scenario	Is this information specific to an individual?	Is the food bank receiving the information directly from the Covered Entity or Business Associate?	Comments and Considerations
Food bank staff are present at a Covered Entity clinic to meet with any patients identified as food insecure: 1. The clinician identifies a patient as food insecure. 2. With the patient's permission, the clinician walks the patient to the food bank representative at the clinic. 3. The food bank representative meets with the patient and discusses how the food bank can help meet the patient's needs.	Yes	No	• The patient has given permission to the clinician to introduce her to the food bank representative and is present during the introduction. The patient shares information about herself with the food bank representative. Because the information comes from the patient and not directly from the Covered Entity, this sharing of information is consistent with HIPAA requirements.
The Covered Entity provider gives the patient information about the type of food box she will need from the food bank. The patient gives that information to the food bank: 1. The provider tells the patient which type of food box to request. This instruction could be verbal, or it could be a written form. 2. The food pantries have pre-set food boxes for specific health conditions or have the flexibility to tailor food boxes to patients' health needs. 3. The patient presents at the food pantry and explains her diagnosis or her diagnosis-related needs for her food box.	Yes	No	• Even if a written form that the Covered Entity gives the patient is color-coded or has individually identifiable patient information (such as an identifier for the patient) the Covered Entity does not disclose information to anyone except the patient. The Covered Entity is not responsible for how the patient chooses to share her information. • Note about "prescriptions" for food: If the food bank fills a "prescription" for a food box, it may be furnishing "health care" within the meaning of HIPAA.[47] Such activity could render the food bank a health care provider.[48] A health care provider that transmits individually identifiable health information in electronic form in connection with a covered transaction is a Covered Entity under HIPAA.[49] Food banks should therefore be cautious about referring to "prescriptions" in the context of their partnerships with Covered Entities, and may consider using the term "voucher" instead. <u>Limitations</u> • The food bank will not be able to conduct outreach to the patient, so it may be difficult to engage patients. • The food bank may not know how many of each type of food box or which food box components to send to individual pantries.

Scenario	Is this information specific to an individual?	Is the food bank receiving the information directly from the Covered Entity or Business Associate?	Comments and Considerations
The Covered Entity provider and food bank share only food box-specific information: 1. The provider sends the food bank an inventory of how many of each type of food box will be needed and to which pantry the food boxes should be distributed. 2. The food bank prepares the food boxes and has them ready at the applicable pantry locations. 3. Patients present at the pantries and request the applicable food box.	No	Yes	• The Covered Entity does not share any individually identifiable health information. <u>Limitations</u> • The food bank will not be able to conduct outreach to the patient, so it may be difficult to engage patients. • The provider would need to keep track of which pantry is most convenient for each patient and ask the food bank to have a certain amount of appropriate inventory at each location. • The patient may not ultimately present at the food bank.
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 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.	Yes	Yes	• Under HIPAA, a Covered Entity can share individually identifiable information pursuant to a written request or authorization from the patient. • The patient can complete the form with the provider at any time. The food bank can even have template authorizations on hand that clients can complete on-site. Food banks can then deliver those authorizations to the clients' health care provider in order to receive information about the patient's dietary needs. • In most cases, health care providers must comply with a patient's request to share her health information as long as it is in writing, is signed by the patient, and clearly specifies the intended recipient of the information.[50]
The food bank signs a Business Associate Agreement with the health care provider: 1. The food bank and the provider organization sign a Business Associate Agreement. 2. The provider organization shares PHI with the food bank. 3. The food bank conducts outreach to patients and prepares food boxes as needed.	Yes	Yes	• The food bank would need to abide by the terms of the Business Associate Agreement. • Complying with a Business Associate Agreement could require a significant investment on the part of the food bank, as well as make the food bank liable for civil and criminal penalties under HIPAA. • Instead of signing a Business Associate Agreement, the food bank could ask the health care provider to have patients complete a disclosure request or authorization form before sharing information.

WHEN MIGHT A FOOD BANK BE SUBJECT TO HIPAA REQUIREMENTS?

A food bank generally does not meet the definition of a Covered Entity or Business Associate and is not subject to HIPAA based on provision of food or general nutrition and food education activities.

However, as the health care landscape shifts and providers and payers recognize the positive impact of having patients receive certain health care services in a community setting, a food bank could step in to fill a perceived community health need (e.g. providing Medical Nutrition Therapy using a Registered Dietitian on the food bank's staff) and begin to look more like a health care Covered Entity or a Business Associate of a Covered Entity.

FOOD BANKS AS HEALTH CARE PROVIDERS/COVERED ENTITIES?

If a food bank falls under the HIPAA definition for "health care provider" and electronically transmits health information in connection with a covered transaction, it may become a Covered Entity and therefore become obligated to comply with HIPAA requirements.

A. Food banks as health care providers

Persons or organizations that (1) are a "provider of services" as defined in specific federal laws; [51] (2) provide medical or health services;[52] or (3) furnish, bill, or are paid for health care in the normal course of business are health care providers under HIPAA.[53]

1. **"Provider of services"**
   Specific providers of services referenced in the HIPAA rules include hospitals, skilled nursing facilities, comprehensive outpatient rehabilitation facilities, home health agencies, hospice programs, and hospital or medical school funds.[54] Food banks are not a "provider of services" under this definition.[55]

2. **Organizations that provide "medical or health services."**
   While most food bank operations would not qualify as "medical or health services," some food banks might perform activities that would fall under this classification. If staff or volunteers[56] of the food bank, and not staff of an external organization, conduct these operations, the food bank may be considered a health care provider under HIPAA. Such operations may include, but are not limited to, services and training related to diabetes management and treatment.[57] Remember that to be a Covered Entity under HIPAA, a food bank must meet the above definition and electronically transmit health information in connection with a covered transaction. A food bank that simply provides diabetes nutritional counseling to a client without transmitting individual client information for billing or other specified purposes is not a Covered Entity.

3. **Furnishing, billing, or being paid for "health care" in the normal course of business**
   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.[58]

A few characteristics of this definition of health care are important for food banks. First, the definition is not exclusive; the rules explicitly state that health care "includes, but is not limited to" the above listed activities.[59] The definition gives examples of health care activities, but activities that are similar to those listed could also be considered health care.

Second, health care includes counseling "with respect to the physical or mental condition . . . of an individual or that affects the structure and function of the body."[60] This definition is extremely broad. The provision of Medical Nutrition Therapy to a client by a Registered Dietitian on the food bank's staff, delivered as a medical service reimbursed by the client's health insurance, would likely meet the definition of health care. It is less clear whether less formal nutritional counseling that does not include health insurance reimbursement would also be included.

Third, health care includes the dispensing of any item "in accordance with a prescription."[61] A food bank that regularly fills "prescriptions" for food boxes could potentially be considered a health care provider under HIPAA. Food banks should consult with an attorney before using the term "prescription" in the context of food banks operations or a health care partnership. An alternative to the term "prescription" that does not appear in the definition of "health care" is voucher.

Again, recall that meeting the definition above is ***not enough*** to qualify the food bank as a Covered Entity if the food bank does not *also* transmit information electronically in connection with a covered transaction.

B. Food banks as Covered Entities

Classification as a health care provider alone is not sufficient to render a food bank a Covered Entity. Only health care providers that transmit health information electronically in connection with a covered transaction are Covered Entities.[62] However, meeting the definition of health care provider means that even one transmission of health information in electronic form in connection with a covered transaction could make a food bank a Covered Entity, triggering the obligation to comply with HIPAA.[63] The covered transactions under HIPAA are:

(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Health care electronic funds transfers (EFT) and remittance advice.
(12) Other transactions that the Secretary may prescribe by regulation. [64]

Most food banks do not transmit health information in connection with these transactions and therefore would not be considered Covered Entity health care providers. However, if – for example - a Registered Dietitian employed by the food bank provided Medical Nutrition Therapy (nutritional counseling) to a food bank client and billed Medicaid or Medicare electronically for that service, the food bank would qualify as a Covered Entity.

Another example of electronic information sharing which may fall into these transactions is returning client information to a health care provider about a particular patient. If a food bank is sending individual client information to a health care provider that contains health data, please see p. 17 on *What it Means to Comply with HIPAA*. Refer to the table on the next page for some sample scenarios that explore the potential classification of food banks as Covered Entity health care providers.





Activities	Is the food bank providing medical or health services or furnishing, billing, or being paid for "health care" in the normal course of business(and therefore a health care provider)?	Is the food bank electronically transmitting health information in connection with a covered transaction?	Conclusion
An external health care provider comes to the food pantry to do blood pressure screening. Patients without a primary care physician are referred to the health care provider's home clinic.	No (in this case the health care provider is doing the screening)	No	The external provider is providing the service, not the food pantry.
Food bank staff offer Diabetes Self-Management Training to clients with diabetes. No summaries are shared with the client's PCP and no insurance billing occurs.	Yes	No	The diabetes management training is likely "medical or health services" and "health care." Because food bank staff provide the training, the food bank meets the definition of health care provider. However, there is no transmission of health information, so the food bank is not a Covered Entity.
Food bank staff receive a referral from a clinic, which has been authorized by the patient. Food bank staff call the patient and offer her the full range of services available at the food bank. Food bank staff respond electronically to the provider to report that they connected with the client and delivered nutritional counseling.	Unclear	Unclear	Nutritional counseling may be considered a "medical or health service" under the very broad definition in HIPAA. Furthermore, although it appears that the information transmitted by the food bank in this scenario does not fall into one of the listed covered transactions on p. 11, the broadness of the definitions make it best to err on the side of caution when communicating health-related, individually identifiable information back to a health care provider.
The food bank staff offer nutrition education classes and learn that a client does not have a doctor. They send a referral to their local community health center to facilitate accessing primary care.	Unclear	No	Depending on whether nutrition education could be classified as "medical or health services" or "health care," the food bank may be considered a health care provider. However, this operation would not make the food bank a Covered Entity because the transmission is not in connection with a covered transaction.[65]
A Registered Dietitian on the food bank's staff offers Medical Nutrition Therapy to a client and sends a claim electronically to Medicaid.	Yes	Yes	The Medical Nutrition Therapy likely falls under the HIPAA definition of "health care." The food bank is therefore a health care provider. The food bank has also transmitted health information in electronic form in connection with a covered transaction (sending a claim). It is therefore a Covered Entity.

Activities	Is the food bank providing medical or health services or furnishing, billing, or being paid for "health care" in the normal course of business(and therefore a health care provider)?	Is the food bank electronically transmitting health information in connection with a covered transaction?	Conclusion
A food pantry regularly fills patients' "prescriptions" from a clinic for food boxes.	Yes	No	The food pantry furnishes health care because it dispenses items in accordance with a prescription.[66] Because it fills these prescriptions in the normal course of business, it may meet the definition of a health care provider.[67] However, because there is no electronic transmission in connection with a covered transaction, the food pantry is therefore not a Covered Entity.
A food pantry regularly fills patients' "vouchers" from a clinic for food boxes.	No	No	Remember that while furnishing an item in accordance with a "prescription" is considered health care, providing a food box in connection with a "voucher" is not.
A food pantry provides specialty food boxes to patients according to color-coded forms the client gives them. The client has received the color-coded form from the clinic. The form indicates what type of meal the patient needs and has an identifying number for the patient. The food pantry then emails the clinic the numbers on the forms the patients provided.	No	No	This operation does not make the food pantry a health care provider under HIPAA. By giving the form to the food bank herself, the patient has chosen to disclose information about her health status. The patient always has the right to disclose her PHI to any third party she chooses. Because providing a food box is not a health or medical service, the food bank is not a health care provider or Covered Entity.

FOOD BANKS AS BUSINESS ASSOCIATES?

Business Associates of Covered Entities also must comply with the requirements of HIPAA rules.[68] A Business Associate of a Covered Entity is a company or organization that is separate from the Covered Entity but that requires PHI in order to conduct activities on behalf of or provide certain services (specifically: legal, actuarial, consulting, data aggregation, management, administrative, financial, or accreditation services) to the Covered Entity.[69]

Covered Entities and their Business Associates must sign written Business Associate Agreements that describe the functions that the Business Associate will carry out for the Covered Entity.[70]

Generally, food banks do not meet the HIPAA definition of "Business Associate."[71] Simply working with a Covered Entity does not make a food bank a Business Associate. Food banks rarely, if ever, perform the services listed in the definition of a Business Associate.[72]

However, performing certain activities or functions **on behalf of** a Covered Entity may make a food bank a Business Associate.[73] Food banks are most likely to engage in activities that could be considered "population-based activities relating to improving health or reducing costs" or "case management."[74] If a food bank contracts with a Covered Entity to provide nutritional advice to diabetic patients, for example, it is performing a service on behalf of a Covered Entity and would therefore meet the definition of Business Associate.[75]

BUSINESS ASSOCIATE AGREEMENTS: WHAT THEY ARE AND WHAT THEY MEAN

A Business Associate Agreement is a contract that a Covered Entity and its Business Associate must sign before sharing protected health information.[76] It is important to remember that unless a food bank takes on activities that make it a Covered Entity or a Business Associate, it is not subject to HIPAA requirements and would not need a Business Associate Agreement or other confidentiality agreement in order to work with Covered Entities.[77] It is the Covered Entity that is responsible for obtaining patient authorization or securing a Business Associate Agreement.

Food banks and food pantries that are neither Covered Entities nor Business Associates are not required to comply with the HIPAA rules and do not need a Business Associate Agreement or other confidentiality agreement in order to work with Covered Entities.[x]

Because Business Associates are directly responsible for complying with the requirements of HIPAA rules, food banks should carefully consider whether signing a Business Associate Agreement is in their best interest.[78] See p. 17, *What it Means to Comply with HIPAA*, to learn more about HIPAA requirements. In lieu of signing a Business Associate Agreement, food banks might encourage a health care partner to obtain individual patient authorization to disclose PHI.

Before agreeing to sign a Business Associate Agreement or any other agreement, it is important for food banks to understand the extent of the responsibilities and legal obligations they incur when signing a contract with a health care partner.

Remember that a Business Associate Agreement, Memorandum of Understanding, or other signed agreement is a contract with which both parties must comply. Moreover, a Business Associate Agreement is a special type of contract that may render the food bank liable under HIPAA for any failures to handle PHI in accordance with the Agreement's terms or HIPAA requirements.

Before a food bank signs any contract, agreement, or Memorandum of Understanding, it must ensure that it can meet the obligations described in the document and is comfortable assuming any responsibilities it might be assigned (such as liability for mishandling patient information). If a food bank cannot meet the obligations as they are written, it must negotiate with the health care partner to alter the language in the contract.

Before signing a Business Associate Agreement:

- **Ask your health care partner whether the goals of the partnership can be met by having the Covered Entity obtain patient disclosure requests or authorizations instead of requiring a Business Associate Agreement.**
- **Read every part of the Business Associate Agreement carefully. If you do not understand the provisions, ask for clarification.**
- **Conduct a realistic assessment of whether your food bank can meet the additional responsibilities and obligations described in the contract. Also see p. 17 on *What it Means to Comply with HIPAA*. If you cannot meet these obligations, do not sign the Business Associate Agreement. Look for a different way to partner with your health care provider.**

- **Consult an attorney. When cost is a factor, look for pro bono legal help from local law firms that are experienced in reviewing contracts.**

Even though food banks typically do not meet the definition of a Business Associate, a Covered Entity may ask a food bank to sign a Business Associate Agreement for two reasons: (1) A Business Associate Agreement allows the Covered Entity to share PHI with the food bank without a patient's authorization or written request; and (2) the Covered Entity is accustomed to signing Business Associate Agreements with other companies and organizations.

A food bank that signs a Business Associate Agreement agrees to take on all of the obligations that the Agreement describes. If a food bank does decide to enter into a Business Associate Agreement, it should make sure that it is familiar with all of the terms of the Agreement and that it can fulfill the obligations that the Agreement assigns to it. Below is an overview of provisions that a Business Associate Agreement must contain (required) and may contain (optional):

A. Required Components of a Business Associate Agreement[79]

A Business Associate Agreement must establish the **permitted uses of PHI** by the Business Associate and the situations in which the Business Associate may disclose PHI to third parties. It must **restrict sharing of the information by the Business Associate** to situations specified in the agreement or as otherwise required by law.

The agreement also must require the Business Associate to **establish safeguards for information**. Such safeguards may include specifying which types of employees will have access to the information, what information they will need to access, and why they will need to access the information in order to do their jobs,[80] as well as providing for secure storage with restricted access to the information and having established processes in place to prevent unauthorized use or disclosure of information.[81] If the information is shared electronically with the Business Associate, the Business Associate must abide by the requirements of the HIPAA Security Rule, which establishes requirements for the protection of PHI stored in electronic form.[82]

Furthermore, under the Business Associate Agreement, the Business Associate must agree to:

- **report any unauthorized use or disclosure of information** (including a breach) to the Covered Entity
- **give PHI to patients upon request**
- **incorporate patient-requested amendments** to their PHI
- **make available to HHS upon request its internal records and practices** relating to the use and disclosure of PHI
- **subject any subcontractors that access PHI to the same restrictions** that the Business Associate has in its Business Associate Agreement
- **enable the Covered Entity to comply with applicable provisions of the Privacy Rule** in sharing PHI, which would require the Business Associate to take actions such as:
    - establishing policies and procedures for disclosures of information and requests for disclosures of information[83]
    - disclosing information to individuals upon request[84]
    - disclosing information to the United States Department of Health and Human Services (HHS) in a compliance investigation or enforcement action[85]
    - implementing reasonable safeguards to prevent unauthorized use or disclosure of information[86]
    - receiving only the minimum necessary information required for its operations,[87] ensuring that its use of the information complies with the Covered Entity's privacy policies[88]
    - maintaining the ability to produce an accounting of disclosures of PHI upon request.[89]

Finally, the Business Associate Agreement must authorize the Covered Entity to terminate the agreement if the Business Associate violates any important provision, including in the event of an unauthorized disclosure of PHI. A provision with this authorization could have a title of **"Termination for cause."** Upon termination of the agreement, the Business Associate must destroy or return to the Covered Entity all PHI it has received from the Business Associate relationship.

B. Optional Components of Business Associate and Confidentiality Agreements[90]

There are other optional provisions that may be included in Business Associate Agreements, although they are not required. The following are areas where you have some leeway to negotiate what obligations and costs you are or are not willing to accept.

An **Indemnification provision**[91] would indicate that the Business Associate would assume all civil liability (including monetary penalties) for an unauthorized use or disclosure of PHI. Food banks should be very cautious about this type

of provision, as it could leave them bearing full monetary responsibility (including both penalties and costs for complying with a government investigation) for a violation of the agreement or HIPAA rules.

A **Survival provision** would indicate that the Business Associate's obligation to safeguard PHI survives the termination of the agreement.

An **Amendment provision** would allow the parties to amend the agreement periodically or as required by changes to the HIPAA rules, and an **Interpretation provision** would specify that if an ambiguous situation arises, the agreement should be interpreted in a manner consistent with the HIPAA rules. These provisions are often included in Business Associate Agreements in order to ensure that they are consistent with the most up-to-date requirements of HIPAA.

Standard agreements that Covered Entities use may contain a **de-identification provision**, which would allow a Business Associate to de-identify PHI for uses such as research.

An agreement could specify the **"minimum necessary"** information or required uses of individually identifiable health information that the Business Associate or community partner will need in order to carry out its functions. This provision could take the form of a list of types of information to which the organization will have access or a list of permitted uses or disclosures of information by the community partner.





WHAT IT MEANS TO COMPLY WITH HIPAA

Complying with HIPAA means abiding by the requirements of HIPAA rules. HIPAA rules require Covered Entities and their Business Associates to take steps to keep individually identifiable health information secure while providing patients with access to their health information.[92] HIPAA also makes Covered Entities and their Business Associates liable for civil and criminal penalties for failing to abide by HIPAA requirements.[93] As a general matter, Covered Entities must ensure compliance with the HIPAA Privacy, Security, and Breach Notification Rules; food banks who are Business Associates must comply with the HIPAA Security Rule and Breach Notification Rule as well as certain provisions of the HIPAA Privacy Rule.[94] For a more detailed description of the specific HIPAA requirements for Business Associates, see Appendix III.

For a food bank to become HIPAA-compliant, it will need to dedicate time and energy to determining what policies and procedures the food bank can reasonably undertake when handling sensitive information. This section will provide an overview of obligations under HIPAA that are relevant to food banks. Food banks that seek to become HIPAA-compliant should be prepared to invest time and resources in order to do the following:

(1) **Assess risk:** Food banks should develop a Security Management Plan to help determine when and how PHI is created, transmitted, and/or received; what the potential risks and vulnerabilities are with respect to unauthorized sharing of this information; ways to mitigate identified risks; and unique characteristics each food bank has that may affect feasibility of the Security Management Plan implementation (e.g., technology infrastructure, size).

(2) **Develop and document policies:** One of the most important aspects of ensuring HIPAA compliance is documenting policies and procedures that the food bank adopts to protect PHI.[95] Food banks must document the rationale for rejecting or selecting certain policies and procedures. They must also document their experiences with implementing the chosen policies and procedures, and periodically review and update them to ensure that the policies are responsive to any changes either in the law or in the food bank's collaborations or internal practices.

(3) **Train staff:** Food banks must develop training materials that inform all workforce members about HIPAA and relevant HIPAA-related policies and procedures. All workforce members (employees, volunteers, and contractors supporting the food bank) should be trained periodically, with special and more frequent training given to staff who will interact with PHI.

(4) **Invest in physical safeguards and technology to protect PHI:** Food banks that seek to become HIPAA-compliant may need to invest in equipment, technology, software, new locks, and other physical measures to be sure they are following HIPAA rules. Although the rules allow organizations to tailor their risk mitigation strategies to their unique circumstances, food banks should still take all requirements seriously and allocate some funding for complying with their HIPAA obligations.

The federal Office of the National Coordinator for Health Information Technology (ONC) recommends that organizations develop a Security Management Plan in order to ensure that they have considered and implemented policies that respond to all HIPAA requirements.[96] Template instructions for developing a Security Management Plan are below. Remember that each food bank's Security Management Plan will be unique to the needs and capacity of the organization. Always seek individual legal guidance to ensure that a Security Management Plan is complete.

FOUR STEPS TO DEVELOPING A SECURITY MANAGEMENT PLAN FOR BUSINESS ASSOCIATES

The overview below is adapted from the ONC's "Sample Seven-Step Approach for Implementing a Security Management Process."[97] It is not intended to be exhaustive; rather, it should serve as a starting point for food banks looking to take short- and long-term steps towards becoming HIPAA-compliant.

STEP 1: CONDUCT A RISK ANALYSIS

A food bank will begin the process of developing a Security Management Plan by conducting a comprehensive risk analysis. To do this, the food bank will designate a security

officer, preview their security risk, review the existing policies and procedures to protect PHI (if any), and document the process and findings of the risk analysis.

Designate a security officer. A designated security officer will be responsible for developing and documenting all of the HIPAA-related policies and procedures as well as ensuring that the food bank remains HIPAA-compliant. The security officer should use all available resources to develop a full understanding of the HIPAA rules. For example, the Office of the National Coordinator for Health Information Technology and the Department of Health and Human Services make the following resources available:

- Regional Extension Centers assistance[98]
- Office of the National Coordinator for Health Information Technology (ONC) Health IT Privacy and Security Resources web page[99]
- Office for Civil Rights Security Rule Guidance Material[100]
- Office for Civil Rights audit protocols[101]

Use tools to preview your security risk. ONC has a series of online resources to help organizations assess risk when it comes to protecting and managing PHI.[102] A food bank can use the Security Risk Assessment tool, which is designed to take an organization through each HIPAA requirement by presenting a question about the organization's activities in the form of "yes" or "no" questions and then showing if a corrective action is needed for that particular item.[103] Keep any and all results as part of the food bank's documentation.

Review the food bank's existing security measures to protect electronic PHI, if any. The risk analysis process identifies and assesses potential threats and vulnerabilities to confidentiality, integrity, and availability of electronic PHI. You will use the results of the risk analysis to inform your risk mitigation action plan (see more information on risk mitigation in Step 2.)

A food bank's first comprehensive security risk analysis should:

- Identify where electronic PHI exists, including how it is created, received, and transmitted.
- Identify potential threats and vulnerabilities. Examples of threats include human threats such as cyberattack, theft, or workforce member error; natural threats, such as earthquake, fire, or tornado; and environmental threats, such as pollution or power loss. Vulnerabilities are flaws or weaknesses that if exploited by a threat could result in a security incident or a violation of policies.
- Assign a level to each identified risk (e.g., high, medium, low). Assess the potential impact of each threat to the confidentiality, integrity, and availability of electronic PHI.

Document the food bank's process, findings, and actions. Documentation is a requirement under the HIPAA Security Rule.[104] Comprehensive documentation will show how the security analysis was conducted and what safeguards were implemented. It should include, but is not limited to, the following:[105]

- Organization's policies and procedures
- Completed security checklists
- Training materials presented to staff and volunteers as well as any associated certificates of completion
- Updated Business Associate Agreements
- Security risk analysis reports
- Technology audit logs that show utilization of security features and monitoring of users' actions
- Risk management action plan or other documentation, implementation timetables, and implementation notes
- Security incident and breach information

STEP 2: DEVELOP AN ACTION PLAN TO PROTECT PHI AND MITIGATE RISK

Develop an action plan. Using the results of the risk analysis, discuss and develop an action plan to mitigate the identified risks. The action plan should have five components: administrative safeguards,[106] physical safeguards,[107] technical safeguards,[108] organizational standards,[109] and policies and procedures.[110] (See Appendix III for a more detailed discussion of each component). The Table below includes sample vulnerabilities and security mitigation strategies related to each component. An effective action plan will take identified vulnerabilities, document appropriate security mitigation strategies and their rationales, and include a plan for implementation.

Adapted from "Five Security Components for Risk Management." Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. 45 (April 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

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

Convene a team. The security officer should convene a team responsible for developing the risk mitigation action plan. The team should include representatives from parts of the food bank that deal with electronic PHI to understand the ways in which they create, use, and transmit PHI. The team should begin first by identifying what are the simplest actions that can reduce the greatest risks. For example, a food bank may only have a small subgroup of employees that handle electronic PHI. As part of the technical safeguards component of the food bank's plan, the food bank can employ secure user IDs, passwords, and appropriate role-based access to certain electronic files so that these individuals are the only staff members who have access to PHI. Once the plan is complete, the designated security team should meet periodically to coordinate actions, work through unexpected issues, and track progress.

Decide what security strategies to use. Every organization may not have the capacity to use complex or expensive technology platforms to handle PHI. A food bank must decide what security strategies will be most effective in protecting PHI and most realistic for the food bank to adopt. The HIPAA Security Rule lays out the following four factors that must be considered when designing a security management plan:[111]

- the size, complexity, and capabilities of your organization;
- the technical infrastructure, hardware, and software security capabilities of your organization;
- the costs of security measures; and
- the probability and criticality of potential risks to electronic PHI.

Assessing risk and capacity – an example.

The HIPAA Security Rule asks an organization to explore encryption of electronic PHI and determine whether or not it is a reasonable and appropriate safeguard for the information's confidentiality, integrity, and availability. The food bank must consider whether purchasing or obtaining the technology to encrypt any PHI it may hold or encounter is feasible based on the factors above. If encryption will be costly and the amount of electronic PHI that a food bank encounters or holds is relatively small, the food bank might choose not to obtain encryption technology. It must document the rationale for this choice and adopt other risk mitigation strategies that are more appropriate for the food bank's capacity and the vulnerability of the PHI.

It is important to note that for any single risk, a combination of safeguards may be used to mitigate vulnerabilities. For example, to ensure appropriate and continuous access to patient information,[112] a food bank might improve the physical safeguards to PHI by adding a power surge protection strip, putting the server in a locked room, and being meticulous about backups.

Examples of simple low-cost, highly effective safeguards[113]

- Say "no" to staff requests to take home laptops containing unencrypted electronic PHI.
- Remove hard drives from old computers before you get rid of them.
- Do not email electronic PHI unless you know the data is encrypted or you are using a secure HIPAA-compliant portal.
- Make sure your server is in a room accessible only to authorized staff, and keep the door locked.
- Make sure the entire office understands that passwords should not be shared or easy to guess.
- Maintain a working fire extinguisher in case of fire.
- Check your servers often for viruses and malware.

Written Policies and Procedures [114]

Written policies and procedures should, at a minimum:

- Establish protocols for all five security components listed in the table on p. 19.
- Commit to a HIPAA training program for all new staff when they are hired and on a regular basis for the entire workforce.
- Instruct your workforce on what to do as part of "incident responses" or "breach notification and management" plans.
- Specify a sanction policy for violations.
- Detail enforcement, starting with the use of security audit logs to monitor access, use, and disclosure of electronic PHI.

Once your policies and procedures are in place, HIPAA rules require that your organization:

- Trains its workforce on what is required and how to implement the policies and procedures, including breach notification.[115]
- Consistently apply your policies and procedures when unauthorized access to PHI occurs.[116]
- Periodically review your policies and procedures to make sure they are current and your practice adheres to them.[117]

Retain your policies and procedures in your documentation folder at least six years after you have updated or replaced them. (State requirements may specify a longer time period).[118]

STEP 3: IMPLEMENT ACTION PLAN TO PROTECT PHI

Implement the action plan. The implementation of the security management plan should be documented throughout the process. Again, the process for each food bank will differ based on the unique nature of PHI data at the food bank, the needs of the organization as a whole, the size and complexity of the food bank, and other characteristics of the organization.

Prevent breaches by educating and training your workforce. Workforce education and training — plus a culture that values patients' privacy — are a necessary part of risk management. All of the food bank's workforce members — employees, volunteers, trainees, and contractors supporting your office — need to know how to safeguard patient information.[119] The training program should prepare the food bank workforce to carry out:

- Individual roles and responsibilities in safeguarding patients' health information and complying with the HIPAA Rules;
- The food bank's HIPAA-related policies; and
- The food bank's procedures, including processes to monitor security and steps for breach notifications.

HIPAA training should be part of all new employee, contractor, or volunteer on-boarding. Additionally, industry best practices suggest that the entire workforce should be trained at least once a year and any time the food bank changes its policies, procedures, systems, location, or infrastructure. In particular, the workforce should be trained on how to respond immediately and appropriately to any potential security incidents or an unauthorized disclosure of electronic PHI because these situations may constitute of a breach of information. (For more information about what to do in event of a breach, see Appendix III).

Update your Business Associate Agreements. Be sure that Business Associate Agreements accurately reflect the food bank's responsibilities and capacity. Update the Agreements regularly to reflect changes in procedure or project protocol.

STEP 4: REVIEW AND UPDATE THE RISK MITIGATION ACTION PLAN PERIODICALLY

Monitor, audit, and update security stratregies on an ongoing basis. The HIPAA Security Rule requires organizations to have audit controls in place and have the capability to conduct an audit. HIPAA asks organizations to "audit" in two ways: 1) monitor the adequacy and effectiveness of your security infrastructure and make needed changes,[120] and 2) examine what happens to PHI within the organization. This means that the technology your food bank employs should be set up to maintain retrospective documentation — or an audit log — on who, what, when, where, and how an individual's PHI has been accessed.[121] Audit control and capabilities should again be scaled to the size of the organization.





CONCLUSION

Together, food banks and their health care partners can promote the health and well-being of the populations they serve. Food banks have an integral role to play in ensuring that clients have access to the food they need in order to stay healthy.

Forging successful partnerships requires understanding the legal responsibilities of all parties involved, including the obligations for protecting health information that HIPAA places on Covered Entities and their Business Associates. While the considerations surrounding these working relationships are complex, partnerships between food banks and health care will help individuals who are food insecure live healthier lives. Navigating HIPAA and other barriers in order to collaborate is worth the investment. By working together, food banks and the health care system can fulfill their respective missions to ensure that people are nourished and communities are healthy and strong.



APPENDIX I: PATIENT'S WRITTEN AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

A valid written authorization must include (1) a specific and meaningful description of the information to be shared, (2) an identification of the person or entity authorized to make the disclosure, (3) an identification of the recipient of the information, (4) an expiration date or event for the authorization, and (5) the patient's signature and the date.[122] The authorization also must inform the patient of (1) her right to revoke the authorization in writing and any exceptions to or limitations of that right, (2) whether and to what extent the Covered Entity can condition the provision of services to the patient on signing the authorization, and (3) the risk that the recipient may redisclose the information and not be subject to HIPAA requirements or penalties.[123] Finally, the authorization must be written in plain language, and the Covered Entity must give a copy of the authorization to the patient.[124] State laws and regulations may impose additional requirements or restrictions on written authorizations.[125]

Patient Authorization to Disclose Health Information

A copy of this completed form must be provided to the patient

Pursuant to the Health Insurance Portability and Accountability Act, 45 C.F.R. Parts 160, 164

1. Authorization

   I hereby authorize _____ (HIPAA Covered Entity, hereafter known as COVERED ENTITY) to disclose protected health information as described below to _____ (Food Bank, hereafter known as RECIPIENT).

2. Effective Period

   This authorization for release of information covers health information from:
   a. ☐ all past, present, and future time periods
      OR
   b. ☐_____ to _____

3. Extent of Authorization

   I authorize the release of my information in my health record related to diet and nutrition needs with the exception of the following information (check all that apply):

   ☐ Mental health records
   ☐ Communicable diseases including HIV and AIDS
   ☐ Treatment for alcohol or drug abuse
   ☐ Other (please specify): _____

4. Use of Information

   I understand that RECIPIENT will use my information in order to assist me with managing my dietary needs, including as they relate to my health care needs.

5. Expiration

   This authorization shall remain valid until _____ (date or event), at which time it will expire.

6. Right to Revoke

   I understand that I may revoke this authorization in writing at any time before it expires. However, I also understand that my revocation will not apply to any disclosure of my health information made in reliance on this authorization

before COVERED ENTITY has received my revocation.

7. Condition of Provision of Services

   COVERED ENTITY may not condition the provision of services on my completion of this authorization. However, I understand that this authorization is required for COVERED ENTITY to share my health information with RECIPIENT.

8. Risk of Redisclosure

   I understand that after releasing my information in accordance with this authorization, COVERED ENTITY is not responsible for any subsequent uses or disclosures of my information by RECIPIENT or any other entity or individual. RECIPIENT may not be subject to HIPAA.

9. Signature

   Patient Signature_____ Date _____

   OR

   Name of Patient's Representative (print) _____

   Signature of Patient's Representative _____ Date _____

   Authority to Sign for Patient: _____

APPENDIX II: BUSINESS ASSOCIATE AGREEMENT

Business Associate Agreement Template

This template agreement with explanatory annotations is based on the sample Business Associate Agreement available from the U.S. Department of Health and Human Services Office for Civil Rights. Each section can be tailored to the needs of a food bank and its health care partner. Many health care partners may already have their own template Business Associate Agreements that they will want to use for a potential partnership. Food banks should read these Agreements carefully and ask for clarification or amendments to any terms they do not understand or with which they cannot or do not want to comply.

Food banks should exercise caution before signing Business Associate Agreements, as signing a Business Associate Agreement may give the food bank a legal obligation to comply with all applicable HIPAA requirements. As an alternative to using a Business Associate Agreement, food banks and their health care partners can share health information by obtaining authorizations from the patient herself.

The provisions below are required to appear in a valid Business Associate Agreement in some form unless otherwise noted.

AGREEMENT BETWEEN _____HEALTH CARE ENTITY_____ AND _____FOOD BANK_____ TO COORDINATE WITH _____HEALTH CARE ENTITY_____ TO IDENTIFY AND SERVE PATIENTS WITH NUTRITION NEEDS

Definitions

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____FOOD BANK_____. _____FOOD BANK_____ assumes the responsibilities of this agreement and the responsibilities required by law of Business Associates to the extent that it meets the definition of the term "Business Associate" at 45 CFR 160.103.

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____HEALTH CARE ENTITY_____.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

Appropriate safeguards under HIPAA rules (45 CFR 164.530) are administrative, technical, and physical measures that reasonably protect individually identifiable health information from impermissible use or disclosure. For a food bank that stores this information in paper form, an appropriate safeguard could be a locked file closet that has access limited by a key held only by certain individuals. The food bank would need to have its privacy procedures documented, train its staff on those practices, and maintain an accounting of all disclosures of protected health information.

If the food bank keeps protected health information in electronic form, it must comply with the requirements of the HIPAA Security Rule, which establishes security standards for protected health information in electronic form. For details regarding the requirements of the Security Rule and other HIPAA Rules, refer to the section of the resource with the title, "What It Means to Comply with HIPAA."

(c) Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(e) Make available protected health information in a designated record set to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;

45 CFR 164.524 requires Covered Entities to make available to individuals upon request access to their protected health information held in a designated record set. A designated record set is a group of records that is maintained by or for a Covered Entity that pertains to medical, billing, enrollment, payment, or claims information or that the Covered Entity uses to make decisions about individual patients. This provision means that a food bank will make the protected health information it maintains available to the Covered Entity in order to fulfill a patient's request for information.

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the Covered Entity or by the patient pursuant to 45 CFR 164.526;

(g) Maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528, or, in response to a request of an accounting of disclosures directly from an individual, to the individual;

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

Subpart E of 45 CFR Part 164 pertains to: uses and disclosures of protected health information; providing patients with notice of the Covered Entity's privacy practices and procedures; patients' right of access to their protected health information; patients' right to amend their protected health information; patients' right to an accounting of the disclosures of their protected health information; and administrative safeguards for keeping protected health information secure (including training of personnel on privacy policies and procedures). This provision would apply to a Business Associate if it performs functions such as maintaining accountings of information disclosure, incorporating patient-requested amendments to their information, or implementing safeguards to keep the Covered Entity's protected health information secure. Food banks are unlikely to take on these responsibilities for Covered Entities.

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

In practice, this means that a food bank must have documented procedures for keeping protected health information secure and must keep an accounting of all disclosures of protected health information. The food bank must keep this information in order to report it to the Secretary of Health and Human Services in the event of a compliance investigation.

Permitted Uses and Disclosures by Business Associate

(a) Business Associate may only use or disclose protected health information:

1. to assist patients of Covered Entity with meeting their nutritional and health needs, which may include contacting patients, distributing food to patients according to their health needs, advising patients about the location(s) where they can most conveniently obtain nutritional assistance and the services they will be able to obtain at the location(s), and referring patients to other health care providers for the purposes of receiving services the food bank does not provide.
2. to assist Covered Entity with its health care operations, including population health activities aimed at improving health or reducing health care costs, which may include use of protected health information to monitor patient activity and utilization of services at any and all locations of Business Associate and to report the details of such activity and utilization to Covered Entity or other health care providers for the purposes of treatment.
3. as required by law.
4. as required by Covered Entity's minimum necessary policies and procedures that have been provided to the Business Associate and are attached to this Agreement.
5. for the proper management and administration of the Business Associate or to carry out the legal

responsibilities of the Business Associate.

6. to provide data aggregation services relating to the health care operations of the Covered Entity.

In addition to other permissible purposes, Business Associate may de-identify protected health information in accordance with 45 CFR 164.514(a)-(c). Because health information that is de-identified in accordance with 45 CFR 164.514(a)-(c) is not protected health information, Business Associate may disclose such information to Covered Entity or other individuals or entities that are not parties to this agreement.

(b) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity.

This provision effectively means that the Business Associate may not disclose protected health information to third parties without the patient's valid written authorization, except for purposes permitted by HIPAA rules (which include disclosures to the individual and disclosures for treatment, payment, or health care operations).

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) *[Optional]* Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.

(b) *[Optional]* Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.

(c) *[Optional]* Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

While these are optional clauses in a Business Associate Agreement, they each require the Covered Entity to provide the food bank with important information that may be relevant to the food bank's policies and procedures.

Permissible Requests by Covered Entity

[Optional] Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity, except as such use or disclosure relates to data aggregation, management and administration of the operations of the Business Associate or Covered Entity, and the legal responsibilities of the Business Associate.

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of _____ [Insert effective date], and shall terminate on _____ [Insert termination date or event] or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity.

Covered Entity authorizes termination of this Agreement by Business Associate, if Business Associate determines Covered Entity has violated a material term of the Agreement and Covered Entity has not cured the breach or ended the violation within the time specified by Business Associate.

(c) Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, Business Associate, with respect to protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Destroy or return to Covered Entity the remaining protected health information that the Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as Business Associate retains the protected health information;
4. Not use or disclose the protected health information retained by Business Associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out in the section of this Agreement with the title "Permitted Uses and Disclosures By Business Associate" which applied prior to termination; and
5. Destroy or Return to Covered Entity the protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

(d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

Miscellaneous

(a) *[Optional]* Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) *[Optional]* Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) *[Optional]* Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Signatures

Name: _____ (Food Bank Representative)

Signature: _____ (Food Bank Representative)

Name: _____ (Covered Entity Representative)

Signature: _____ (Covered Entity Representative)

APPENDIX III:

Requirements Under the HIPAA Security Rule for Covered Entities and Business Associates

This overview of the Security Rule is adapted from information provided by the U.S. Department of Health & Human Services.[126]

The Security Rule establishes minimum security standards for protecting all electronic PHI that Covered Entities and their Business Associates create, receive, maintain, or transmit. This requires that organizations:

- ensure the confidentiality, integrity, and availability[127] of all electronic PHI they create, receive, maintain or transmit;
- identify and protect against reasonably anticipated threats to the security or integrity of the information; and
- protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance by their workforce.[128]

The Security Rule also asks Covered Entities and their Business Associates to put in place specific safeguards:

Administrative Safeguards

Security Management Process. The Security Rule is designed to allow organizations to take into account their organization's size, complexity, and other factors as it determines what processes to implement.[129] Thus, an effective risk analysis will be tailored to the needs of each organization.

A central component of the security management process is the risk analysis and management process. Examples of activities this process could include are: evaluating the likelihood and impact of potential risks to electronic PHI ahead of time;[130] implementing appropriate security measures to address the risks identified in the risk analysis, like encrypting information;[131] documenting what security measures are chosen and the rationale for adopting those measures;[132] and ensuring that security protections are maintained.[133] HHS encourages organizations to make risk analysis an ongoing, iterative process.[134]

Security Personnel. A Covered Entity or Business Associate must designate a security official responsible for developing and implementing security policies and procedures. [135]

Information Access Management. A Covered Entity or Business Associate must implement policies and procedures for "minimum necessary" role-based access.[136]

Workforce Training and Management. A Covered Entity or Business Associate must train all workforce members regarding what security policies and procedures it has in place.[137] It must also have sanctions in place for individuals that violate them.[138]

Evaluation. A Covered Entity or Business Associate must perform a periodic assessment to ensure that its policies are complying with the requirements of the Security Rule.[139]

Physical Safeguards

Facility Access and Control. A Covered Entity or Business Associate must limit unauthorized, physical access to its facilities.[140]

Workstation and Device Security. A Covered Entity or Business Associate must implement policies and procedures for the transfer, removal, disposal, and re-use of information.[141]

Technical Safeguards

Access Control. A Covered Entity or Business Associate must implement technical policies and procedures that allow only authorized access to electronic PHI.[142]

Audit Controls. A Covered Entity must put in place mechanisms to record and examine information systems that contain or use electronic PHI.[143]

Integrity Controls. A Covered Entity or Business Associate must implement policies and procedures to ensure and confirm that electronic PHI is not improperly altered or destroyed. [144]

Transmission Security. A Covered Entity or Business Associate must prevent unauthorized access to PHI transmitted over a network.[145]

Policies and Procedures and Documentation Requirements

Policies and Procedures. A Covered Entity or Business Associate must adopt "reasonable and appropriate" policies and procedures based on consideration of the following four factors:[146]

- the size, complexity, and capabilities of your organization;
- the technical infrastructure, hardware, and software security capabilities of your organization;
- the costs of security measures; and
- the probability and criticality of potential risks to electronic PHI.

Documentation. A Covered Entity or Business Associate must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.[147]

Updates. A Covered Entity or Business Associate must periodically review and update documentation as changes that affect the security of electronic PHI occur.[148]

Requirements under Breach Notification Rule for Covered Entities and Business Associates
This overview is adapted from information provided by the Department of Health & Human Services. [149]

Breach. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.[150] Two types of PHI are relevant here:[151]

- Unsecured PHI: An unauthorized person cannot use, read, or decipher any PHI that this person obtains because your organization meets applicable federal standards by encrypting information; clearing, purging, or destroying media that stored or recorded PHI; or shredding or otherwise destroying paper PHI.
- Unauthorized PHI: An unauthorized person may use, read, and decipher PHI that this person obtains because your organization does not encrypt or destroy the PHI; or encrypts PHI, but the decryption key has also been breached.

If a breach is suspected or detected, the Covered Entity or Business Associate should undertake a risk assessment. A risk assessment involves thoroughly assessing at least the following required elements:[152]

1. The nature and extent of the PHI involved in the use or disclosure, including the types of identifiers and the likelihood that PHI could be re-identified.
2. The unauthorized person who used the PHI or to whom the disclosure was made.
3. The likelihood that any PHI was actually acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.

Throughout, the burden is on the Covered Entity or Business Associate to undertake this risk assessment in good faith and demonstrate that the use or disclosure did not constitute a breach. If the Covered Entity or Business Associate can demonstrate through a risk assessment that there is a low probability of compromised PHI, then notification, discussed below, is not necessary.[153]

Breach Notification. If the Covered Entity or Business Associate cannot demonstrate that there is a low probability of compromised PHI, then Covered Entities or Business Associates must notify individuals and the Secretary of HHS[154] of the loss, theft, or certain other impermissible uses or disclosures of unsecured PHI. If a breach occurs at or by the Business Associate, the Business Associate must notify the Covered Entity without unreasonable delay and no later than 60 days from the discovery[155] of the breach.[156] The Business Associate should provide the Covered Entity with the identification of each individual affected by the breach and any other available information required to be provided by the Covered Entity in its notification to affected individuals. The notification requirements vary with the size of the breach:[157]

—*If a breach of unsecured PHI affects 500 or more individuals,* the Covered Entity or Business Associate must notify the affected individuals, the Secretary, and the media if the breach affects more than 500 residents of a state or jurisdiction.

—*If a breach of unsecured PHI affects fewer than 500 individuals,* the Covered Entity or Business Associate must notify the Secretary and affected individuals, with reports due to the Secretary no later than 60 days after the end of the calendar year in which the breach occurred.

Requirements for Business Associates under Privacy Rule

This overview is adapted from information provided by the Department of Health & Human Services.[158]

Business Associates must comply with Privacy Rule requirements to the extent that the Business Associate is carrying out a Covered Entity's Privacy Rule obligations.[159] The contours of this will be dictated by the Business Associate Agreements. For example, if a Covered Entity delegates a Privacy Rule obligation to the Business Associate (e.g., providing a notice of privacy practices for PHI to individuals), Business Associates will need to do so in compliance with the Privacy Rule. As such, a review of existing Business Associate Agreements and a determination regarding future Business Associate Agreements will be required to determine what obligations Business Associates have under the Privacy Rule.

ENDNOTES

[1] Hereafter, all information that applies to "food banks" applies to "food pantries" as well; although only the term "food banks" will be used, it should be understood to incorporate food pantries.

[2] Center for Health Law and Policy Innovation of Harvard Law School & Feeding America, *Food Banks as Partners in Health Promotion: Creating Connections for Client & Community Health* 4 (Jul. 2015), http://healthyfoodbankhub.feedingamerica.org/resource/food-banks-as-partners-in-health-promotion/.

[3] Center for Health Law and Policy Innovation of Harvard Law School & Feeding America, *Food Banks as Partners in Health Promotion: Creating Connections for Client & Community Health* 4 (Jul. 2015), http://healthyfoodbankhub.feedingamerica.org/resource/food-banks-as-partners-in-health-promotion/ (citing Feeding America, Hunger in America: 2014 National Report 118 (2014), http://help.feedingamerica.org/HungerInAmerica/hunger-in-america-2014-full-report.pdf).

[4] Id.

[5] *See, e.g.*, Centers for Disease Control and Prevention, *Social Determinants of Health: Know What Affects Health—Frequently Asked Questions* (Oct. 19, 2015), http://www.cdc.gov/socialdeterminants/faqs/index.htm; Harry J. Heiman & Samantha Artiga, *Beyond Health Care: The Role of Social Determinants in Promoting Health and Health Equity,* The Kaiser Family Foundation (Nov. 4, 2015), http://kff.org/disparities-policy/issue-brief/beyond-health-care-the-role-of-social-determinants-in-promoting-health-and-health-equity/.

[6] Center for Health Law and Policy Innovation of Harvard Law School & Feeding America, *Food Banks as Partners in Health Promotion: Creating Connections for Client & Community Health* 6–11 (Jul. 2015), http://healthyfoodbankhub.feedingamerica.org/resource/food-banks-as-partners-in-health-promotion/.

[7] American Academy of Pediatrics, Council on Community Pediatrics, Committee on Nutrition, *Promoting Food Security for All Children*, 136(5) Pediatrics e1431, e1431 (Dec. 2015), http://pediatrics.aappublications.org/content/pediatrics/early/2015/10/20/peds.2015-3301.full.pdf.

[8] American Diabetes Association, *Diabetes Care: Standards of Medical Care in Diabetes—2016*, 39(1) J. of Clinical and Applied Res. and Educ. S1, S9 (Dec. 22, 2015), http://care.diabetesjournals.org/content/suppl/2015/12/21/39.Supplement_1.DC2/2016-Standards-of-Care.pdf.

[9] *See, e.g.*, American Academy of Pediatrics, Council on Community Pediatrics, Committee on Nutrition, *Promoting Food Security for All Children*, 136(5) Pediatrics e1431, e1435 (Dec. 2015), http://pediatrics.aappublications.org/content/pediatrics/early/2015/10/20/peds.2015-3301.full.pdf; American Diabetes Association, *Diabetes Care: Standards of Medical Care in Diabetes—2016*, 39(1) J. of Clinical and Applied Res. and Educ. S1, S9 (Dec. 22, 2015), http://care.diabetesjournals.org/content/suppl/2015/12/21/39.Supplement_1.DC2/2016-Standards-of-Care.pdf.

[10] Sandra Stenmark et al. *Linking the Clinical Experience to Community Resources to Address Hunger in Colorado,* Health Affairs Blog (Jul. 13, 2015), http://healthaffairs.org/blog/2015/07/13/linking-the-clinical-experience-to-community-resources-to-address-hunger-in-colorado/.

[11] Pub. L. 104-191, 42 U.S.C. § 1320d-5–d-6 (1996).

[12] These regulations are the Privacy Rule, the Security Rule, the Enforcement Rule, and the Final Omnibus Rule. HHS Office for Civil Rights, *HIPAA for Professionals,* http://www.hhs.gov/hipaa/for-professionals/index.html (last visited Sept. 22, 2016).

[13] HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 1 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[14] HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 2–4 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[15] Id.

[16] Id.

[17] HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 2–3 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[18] HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 3 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[19] *See* 45 C.F.R. § 164.524; 45 C.F.R. § 164.502(a)(1)(iv).

[20] Id.

[21] *See* 45 C.F.R. § 164.501 (including "population-based activities relating to improving health or reducing health care costs" in the definition of "health care operations").

[22] HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 2–3 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[23] HHS Office for Civil Rights, *Covered Entities and Business Associates*, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sept. 23, 2016).

[24] Id.

[25] *See* Office of the National Coordinator for Health Information Technology, *Interstate Disclosure*, HealthIT.gov https://www.healthit.gov/policy-researchers-implementers/interstate-disclosure (last visited Oct. 5, 2016).

[26] It is also important to note that as food security and nutrition become integrated into the provision of health care in the United States, food banks and the services they provide may be increasingly regarded as within the scope of "health care." Such a conception, while perhaps not representative of the current state of the health care industry, would introduce additional complexity into the analysis of whether a food bank is (or should be) covered by HIPAA. This resource will provide examples based on currently available information, but future information and developments in the regulation of health information could affect the analysis provided here.

[27] *See* HHS Office for Civil Rights, *Why is the HIPAA Privacy Rule needed?*, http://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html (last visited Oct. 5, 2016).

[28] Id.

[29] *See* Pub. L. 104-191, 42 U.S.C. § 1320d-5–d-6 (1996).

[30] Id.

[31] HHS Office for Civil Rights, *HIPAA for Professionals*, http://www.hhs.gov/hipaa/for-professionals/index.html (last visited Sept. 22, 2016).

[32] Id.

[33] *See* Pub. L. 111-5 (2009).

[34] HHS Office for Civil Rights, *The HIPAA Enforcement Rule*, http://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html (last visited Sept. 22, 2016); HHS Office for Civil Rights, *HIPAA for Professionals,* http://www.hhs.gov/hipaa/for-professionals/index.html (last visited Sept. 22, 2016).

[35] Id.

[36] HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 3 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[37] 45 C.F.R. § 160.103.

[38] Id.

[39] *See* 45 C.F.R. § 164.524; 45 C.F.R. § 164.502(a)(1)(iv).

[40] *See 45 C.F.R. § 164.524(a). The Covered Entity may charge a reasonable, cost-based fee for complying with the request. See* 45 C.F.R. § 164.524(c)(4).

[41] 45 C.F.R. § 164.524(c)(3)(ii).

[42] Id. Covered Entities must send the information in the form and format requested by the patient, as long as that format is readily producible. Covered Entities may charge a reasonable, cost-based fee to fulfill the request. For more information on a patient's right to access PHI and request that it be sent to a third party, *see* HHS Office for Civil Rights, *Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. § 164.524*, http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/ (last visited Oct. 1, 2016).

[43] *See* 45 C.F.R. § 164.524(b)(2)(i). The Covered Entity may provide the patient with reasons for being unable to act upon the request within thirty days and may extend the timeframe by an additional thirty days. *See* 45 C.F.R. § 164.524(b)(2)(ii). Because the patient has a right under HIPAA to make this request, state law cannot extend the timeframe for Covered Entities to respond. In fact, some states may require Covered Entities to respond in a shorter timeframe. *See* Health Information & the Law, *Individual Access to Medical Records: 50 State Comparison* (2012), http://www.healthinfolaw.org/comparative-

analysis/individual-access-medical-records-50-state-comparison.

44 45 C.F.R. § 164.502(a)(1)(iv).

45 45 C.F.R. § 164.502(a)(1) ("A Covered Entity is *permitted* to use or disclose protected health information . . . ") (emphasis added).

46 *See* 45 C.F.R. § 160.103.

47 *See* 45 C.F.R. § 160.103 (defining "health care" as "care, services, or supplies related to the health of an individual," which includes "[s]ale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.").

48 *See* 45 C.F.R. § 160.103 (including any "person or organization who furnishes, bills, or is paid for health care in the normal course of business" in the definition of "health care provider").

49 Id.

50 *See* 45 C.F.R. § 164.524.

51 Hospitals, critical access hospitals, skilled nursing facilities, comprehensive outpatient rehabilitation facilities, home health agencies, hospice programs, and hospital or medical school funds are considered "providers of services." *See* 45 C.F.R. § 160.103 (referring to 42 U.S.C.A. § 1395x(u) in the definition of "health care provider").

52 The HIPAA Privacy Rule provides an illustrative list of such services. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed Reg. 82462, 82478 (Dec. 28, 2000).

53 45 C.F.R. § 160.103.

54 *See* 45 C.F.R. § 160.103 (referring to 42 U.S.C.A. § 1395x(u) in the definition of "health care provider").

55 *See* 45 C.F.R. § 160.103 (referring to 42 U.S.C.A. § 1395x(u) in the definition of "health care provider").

56 *See* 45 C.F.R. § 160.103 (including volunteers in the definition of "workforce").

57 The HIPAA Privacy Rule provides a more comprehensive, but still merely illustrative, list of such services. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed Reg. 82462, 82478 (Dec. 28, 2000).

58 45 C.F.R. § 160.103.

59 *See* 45 C.F.R. § 160.103.

60 Id.

61 *Id.*

62 Id.

63 *See* 45 C.F.R. § 160.103 (including as a Covered Entity a "health care provider who transmits *any* health information in electronic form in connection with a transaction covered by this subchapter") (emphasis added); *see also* Donald R. Moy, *Are You a Covered Entity Under HIPAA*, Medical Society of the State of New York (Sept. 13, 2002), http://www.mssny.org/MSSNY/Practice_Resources/Legal_Matters/HIPAA_NPI/HIPAA_Privacy_Rule/Covered_Entities/MSSNY/Practice_Resources/Legal_Matters/HIPPA_NPI/HIPAA_Privacy_Rule/Covered_Entities.aspx?hkey=86b36b0f-6825-4c24-a1f0-d1785012a89a ("Note, If a medical practice engages in any electronic transaction (even only one transaction) covered under the Electronic Transaction Standard, then the Privacy Standards in their entirety apply to the medical practice.").

64 45 C.F.R. § 160.103.

65 45 C.F.R. § 160.103; *Referral Certification and Authorization,* Ctrs. for Medicare & Medicaid Srvs. (last visited Dec. 20, 2016).

66 *See* 45 C.F.R. § 160.103.

67 Id.

68 HHS Office for Civil Rights, *Covered Entities and Business Associates,* http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sept. 23, 2016).

69 45 C.F.R. § 160.103.

70 HHS Office for Civil Rights, *Covered Entities and Business Associates*, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sept. 23, 2016).

71 *See* 45 C.F.R. § 160.103.

72 45 C.F.R. § 160.103.

73 *See* 45 C.F.R. § 160.103, § 164.501.

74 Id.

75 *See Permitted Uses and Disclosures: Exchange for Health Care Operations: 45 Code of Regulations (CFR) 164.506(c)(4),* Office of Nat'l Coordinator for Health Information Technology, U.S. Dep't of Health & Human Srvs. Office of Civil Rights (Jan. 2016).

76 HHS Office for Civil Rights, *Covered Entities and Business Associates*, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sept. 23, 2016).

77 Id.

78 Kim Stanger, *Avoiding Business Associate Agreements*, Holland & Hart Health Law Blog (Nov. 26, 2013), https://www.hollandhart.com/avoiding-business-associate-agreements.

79 Unless otherwise cited, information in the section is based on HHS Office for Civil Rights, *Business Associate Contracts* (Jan. 25, 2013), http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html; see also 45 C.F.R. § 164.504(e).

80 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 11 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

81 HHS Office for Civil Rights, *Summary of the HIPAA Security Rule*, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (last visited Sept. 13, 2016).

82 Id.

83 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 11 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

84 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 4 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

85 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 4 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

86 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 6 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

87 Id.

88 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 11 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

89 HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 13 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

90 Unless otherwise cited, information in the section is based on HHS Office for Civil Rights, *Business Associate Contracts* (Jan. 25, 2013), http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html; see also 45 C.F.R. § 164.504(e).

91 HHS guidance on Business Associate contracts does not reference indemnification provisions, but it is important for food banks and food pantries to understand what they mean in case they are asked to sign an agreement that contains such a provision. The American Health Information Management Association (AHIMA) has advised Covered Entities to consider including indemnification provisions in their Business Associate Agreements. *See* AHIMA Staff, *Avoiding Liability for Business Associates' Breaches: Adjustments and Ongoing Strategies,* AHIMA.org (Jan. 31, 2014), http://journal.ahima.org/2014/01/31/avoiding-liability-for-business-associates-breaches-adjustments-and-ongoing-strategies/.

92 State laws that are more "stringent" than HIPAA continue to apply. See 45 C.F.R. § 160.202; 45 C.F.R. § 160.203.

93 *See* Pub. L. 104-191, 42 U.S.C. § 1320d-5–1320d-6; see also 45 C.F.R. 160 Subpart D.

94 *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e); Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. (April 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. *See also* The HIPAA Privacy Rule, U.S. Dep't of Health & Hum. Serv., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Feb. 26, 2016); The Security Rule, U.S. Dep't of Health & Hum. Serv., http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ (last visited Feb. 26, 2016); Breach Notification Rule, U.S. Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/breach-notification/ (last visited Feb. 26, 2016).

95 *See* 45 C.F.R. § 164.306(d)(3)(ii)(B)(1) (2007); 45 C.F.R. § 164.316(b)(1) (2007).

96 *See* 45 C.F.R. § 164.208(a)(1) (2007).

97 *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e); Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. (April 2015), at 35. https://www.healthit.gov/

sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

98 *See* Regional Extension Centers, HealthIT.gov, https://www.healthit.gov/providers-professionals/regional-extension-centers-recs (last visited Feb. 26, 2017).

99 *See* Health IT Privacy & Security Resources, HealthIT.gov, https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources (last visited Feb. 26, 2017).

100 *See* Security Rule Guidance Material, U.S. Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Feb. 26, 2017).

101 *See* Audit Protocol, U.S. Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html (last visited Feb. 26, 2017).

102 *See* Health IT Privacy & Security Resources, HealthIT.gov, https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources (last visited Feb. 26, 2017).

103 *See* Security Risk Assessment Tool, HealthIT.gov, https://www.healthit.gov/providers-professionals/security-risk-assessment-tool (last visited Feb. 26, 2017).

104 *See* 45 C.F.R. § 164.316 (2007).

105 Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. (April 2015). https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

106 *See* 45 C.F.R. § 164.308 (2007).

107 *See* 45 C.F.R. § 164.310 (2007).

108 *See* 45 C.F.R. § 164.312 (2007).

109 *See* 45 C.F.R. § 164.314 (2007).

110 *See* 45 C.F.R. § 164.316 (2007).

111 45 C.F.R. § 164.306(b)(2) (2007).

112 *See* 45 C.F.R. § 164.310(c) (2007).

113 From the Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. (April 2015). https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

114 From the Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. (April 2015). https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

115 *See* 45 C.F.R. § 164.308(a)(4)(ii)(C)(5)(i) (2007).

116 *See e.g.*, 45 C.F.R. § 164.308(a)(1)(ii)(C) (2007).

117 *See* 45 C.F.R. § 164.316(b)(2)(iii) (2007).

118 *See* 45 C.F.R. § 164.316(b)(2)(i) (2007).

119 *See* 45 C.F.R. § 164.308(a)(4)(ii)(C)(5)(i) (2007).

120 *See* 45 C.F.R. § 164.316(b)(2)(iii) (2007).

121 *See* 45 C.F.R. § 164.312(b) (2007).

122 45 C.F.R. § 164.508(c)(1). If a representative of the patient signs the authorization, the authorization must include a description of the authority of the representative to act on behalf of the patient. 45 C.F.R. § 164.508(c)(1)(vi).

123 45 C.F.R. § 164.508(c)(2).

124 45 C.F.R. § 164.508(c)(3)–(4).

125 *See,* e.g., HHS Office for Civil Rights, *FAQ: Must an authorization include an expiration date?,* http://www.hhs.gov/hipaa/for-professionals/faq/476/must-an-authorization-include-an-expiration-date/index.html (last visited Oct. 1, 2016) (noting that with respect to the expiration of an authorization, "a more restrictive State law would control how long the Authorization is effective").

126 *See* Summary of the HIPAA Security Rule, U.S. Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Feb. 26, 2017).

127 The Security Rule defines: "confidentiality" to mean that electronic PHI is not available or disclosed to unauthorized persons, "integrity" to mean that electronic PHI is not altered or destroyed in an unauthorized manner, and "availability" to mean that electronic PHI is accessible and usable on demand by an authorized person. *See* 45 C.F.R. § 164.304 (2007).

128 *See* 45 C.F.R. § 164.306(a) (2007).

129 *See* 45 C.F.R. § 164.306(b)(2) (2007). *See also* https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

130 *See* 45 C.F.R. § 164.306(b)(iv) (2007).

131 *See* 45 C.F.R. § 164.308(a)(1)(ii)(B) (2007).

132 *See* 45 C.F.R. § 164.306(d)(3)(ii)(B)(1) (2007); 45 C.F.R. § 164.316(b)(1) (2007).

133 *See* 45 C.F.R. § 164.306(e) (2007).

134 *See* 45 C.F.R. § 164.308(a)(1)(ii)(D) (2007); 45 C.F.R. § 164.306(e) (2007); 45 C.F.R. § 164.308(a)(8) (2007); 45 C.F.R. § 164.306(b)(2)(iv) (2007); 45 C.F.R. § 164.306(e) (2007).

135 *See* 45 C.F.R. § 164.308(a)(2) (2007).

136 *See* 45 C.F.R. § 164.308(a)(4)(i) (2007).

137 *See* 45 C.F.R. § 164.308(a)(3) & (4) (2007).

138 *See* 45 C.F.R. § 164.308(a)(5)(i) (2007).

139 *See* 45 C.F.R. § 164.308(a)(8) (2007).

140 *See* 45 C.F.R. § 164.310(a) (2007).

141 *See* 45 C.F.R. §§ 164.310(b–d) (2007).

142 *See* 45 C.F.R. § 164.312(a) (2007).

143 *See* 45 C.F.R. § 164.312(b) (2007).

144 *See* 45 C.F.R. § 164.312(c) (2007).

145 *See* 45 C.F.R. § 164.312(e) (2007).

146 *See* 45 C.F.R. § 164.306(b)(2) (2007).

147 *See* 45 C.F.R. § 164.316 (2007).

148 *See* 45 C.F.R. § 164.316(b)(2)(iii) (2007).

149 *See* Submitting Notice of a Breach to the Secretary, Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017); Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. 35 (April 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

150 *See* 45 C.F.R. § 164.402

151 Guide to Privacy & Security of Electronic Health Info., Off. of Nat'l Coordinator for Health Info. Tech. 58 (April 2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

152 *See* 45 C.F.R. § 164.402(2) (2007).

153 *See* 45 C.F.R. § 164.402(1) (2007). ("Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.").

154 *See* Submitting Notice of a Breach to the Secretary, Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).

155 *See* Business Associates, HITECH, & the Omnibus HIPAA Final Rule, WEDI, 30 http://www.wedi.org/forms/uploadFiles/35FE700000100.filename.7.26_Combined.pdf (last visited Feb. 26, 2017) ("Discovery is when the Business Associate "knew or should have known.").

156 *See* Submitting Notice of a Breach to the Secretary, Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).

157 *See* Submitting Notice of a Breach to the Secretary, Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).

158 *See* Submitting Notice of a Breach to the Secretary, Dep't of Health & Hum. Serv., https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).

159 *See* Business Associates, HITECH, & the Omnibus HIPAA Final Rule, WEDI, 30 http://www.wedi.org/forms/uploadFiles/35FE700000100.filename.7.26_Combined.pdf (last visited Feb. 26, 2017). *See* 45 C.F.R. §164.404(2) (2007). ("…A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity.").

ENDNOTES, TEXT BOXES

i Feeding America, *Hunger in America 2014: National Report* 1 (Aug. 2014), http://help.feedingamerica.org/HungerInAmerica/hunger-in-america-2014-full-report.pdf?s_src=W169ORGSC&s_referrer=google&s_subsrc=http%3A%2F%2Fwww.feedingamerica.org%2Fhunger-in-america%2Fimpact-of-hunger%2F%3Freferrer%3Dhttps%3A%2F%2Fwww.google.com%2F&_ga=1.62810540.1202093907.1474479588.

ii *Report of the Dietary Guidelines Advisory Committee on the Dietary Guidelines for Americans,* Dietary Guidelines Advisory Committee,

2010, (May 2010), http://www.cnpp.usda.gov/sites/default/files/dietary_guidelines_for_americans/2010DGACReport-camera-ready-Jan11-11.pdf; Véronique L. Roger et al., *Heart disease and stroke statistics 2012 update: A report from the American Heart Association,* American Heart Ass'n (2012), http://circ.ahajournals.org/content/125/1/e2.extract; *Statistics About Diabetes,* American Diabetes Ass'n (Jun. 10, 2014), http://www.diabetes.org/diabetes-basics/statistics/; *Overweight and Obesity Facts,* Ctrs. for Disease Control & Prevention, http://www.cdc.gov/obesity/data/facts.html (last visited Jun.23, 2016).

iii Centers for Disease Control and Prevention, *Social Determinants of Health: Know What Affects Health—Frequently Asked Questions* (Oct. 19, 2015), http://www.cdc.gov/socialdeterminants/faqs/index.htm; Harry J. Heiman & Samantha Artiga, *Beyond Health Care: The Role of Social Determinants in Promoting Health and Health Equity,* The Kaiser Family Foundation (Nov. 4, 2015), http://kff.org/disparities-policy/issue-brief/beyond-health-care-the-role-of-social-determinants-in-promoting-health-and-health-equity/.

iv Erin R. Hager et al., *Development and Validity of a 2-Item Screen to Identify Families at Risk for Food Insecurity*, American Academy of Pediatrics (2010), http://pediatrics.aappublications.org/content/126/1/e26.full-text.pdf; American Academy of Pediatrics, Council on Community Pediatrics, Committee on Nutrition, *Promoting Food Security for All Children*, 136(5) Pediatrics e1431, e1435 (Dec. 2015), http://pediatrics.aappublications.org/content/pediatrics/early/2015/10/20/peds.2015-3301.full.pdf.

v Pub. L. 104-191, 42 U.S.C. § 1320d-5–d-6 (1996).

vi HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule 4 (May 2003),* https://www.hhs.gov/sites/default/files/privacysummary.pdf.

vii HHS Office for Civil Rights, *Summary of the HIPAA Privacy Rule* 2–3 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

viii 45 C.F.R. § 164.524(c)(3)(ii); 45 C.F.R. § 164.502(a)(1)(iv).

ix 45 C.F.R. § 164.524(c)(3)(ii).

x 45 C.F.R. § 160.103.



CENTER *for* HEALTH LAW
and POLICY INNOVATION
HARVARD LAW SCHOOL

FEEDING®
AMERICA