Photo courtesy of Feeding America.

FOOD BANKS AS PARTNERS IN HEALTH PROMOTION:

Navigating HIPAA

June 2020

CHLPI CENTER for HEALTH LAW and POLICY INNOVATION
HARVARD LAW SCHOOL

Health Law Lab
CENTER FOR HEALTH LAW AND POLICY INNOVATION
HARVARD LAW SCHOOL

FEEDING AMERICA

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.

CHLPI's Health Law Lab advances health care system efforts to address social determinants of health and health related social needs, improve health equity, and mitigate health disparities.

Feeding America

Feeding America® is the largest domestic hunger-relief organization in the United States. Through a network of 200 food banks and 60,000 food pantries and meal programs, we provide meals to more than 40 million people each year. Feeding America also supports programs that prevent food waste and improve food security among the people we serve; educates the public about the problem of hunger; and advocates for legislation that protects people from going hungry. Individuals, charities, businesses and government all have a role in ending hunger.

Acknowledgements

Food Banks as Partners in Health Promotion: Navigating HIPAA is written by Jarrod Nelson, Sarah Downer, Rachel Landauer, and Morgan Smith. Portions of this resource rely on the 2017 edition, *Food Banks as Partners in Health Promotion: How HIPAA and Concerns about Protecting Patient Information Affect Your Partnership*, written by Gideon Palte, Dalia Deak, Sarah Downer, Katie Garfield, and Kim Prendergast. Additionally, this resource would not have been possible without the insight and experiences shared by many individuals including: Karen Broussard, Second Harvest Food Bank of Central Florida; Nick Davis, Mid-Ohio Food Collective; Joy Goetz, Atlanta Community Food Bank; Jessica Hager, Feeding America; Amy Headings, Mid-Ohio Food Collective; Sarah Huber, Gleaners Food Bank of Indiana; Lynn Knox, Oregon Food Bank; Esther Liew, Houston Food Bank; Sarah Mills, Gleaners Community Food Bank of Southeastern Michigan; Jennifer Parsons, Mid-Ohio Food Collective; Pierre Pendergrass, Centene Corporation; Gita Rampersad, Feeding America; Rachel Stankiewitch, Second Harvest Food Bank of Central Florida; and Reginald Young, Houston Food Bank.

This resource was made possible through the generous support of the Anthem Foundation, the philanthropic arm of Anthem, Inc. As a Leadership Partner, Anthem Foundation proudly supports the Feeding America® network in growing health care partnerships through grants, sponsorships, and employee matching gift and volunteer programs. Learn more about the Anthem Foundation at www.anthemcorporateresponsibility.com/cr/foundation/.

Report design by Najeema Holas-Huggins.

TABLE OF CONTENTS

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 facing food insecurity and who have, or are at risk for, certain health conditions.

Nutrition affects the onset, management, and outcome of many health conditions, including but not limited to: diabetes, kidney disease, heart disease, stroke, certain cancers, obesity, and HIV.[2]

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) are increasingly focused on addressing social determinants of health—conditions in the places where people live, work, and learn that affect their overall health.[3] Food banks have valuable expertise in addressing food insecurity, one social determinant of health, and supporting people in meeting nutritional needs, and other food-related determinants that impact health outcomes. By working together, food banks and health care can complement each other's expertise with tangible benefits for patients.

Food banks across the country partner with local health care providers and payers to ensure that clients and patients with health concerns have access to healthy, nutritious foods. However, these collaborations between food banks and health care 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 and payers are legally required to keep patient information private and secure. Federal legal obligations have been embodied in federal law through the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and implementing regulations[4] (referred to collectively as "HIPAA" in this resource). HIPAA seeks to encourage the exchange of patient information in order to improve care while ensuring that this information remains protected and private.[5] There is no equivalent law to HIPAA that governs how food banks must handle client information. (However, food banks have always been aware of the need to respect the privacy and dignity of their clients by handling client information carefully, and some states may regulate how food banks use and protect consumer information more generally.)

In 2017, Feeding America and CHLPI published *Food Banks as Partners in Health Promotion: How HIPAA and Concerns about Protecting Patient Information Affect Your Partnership*. The 2017 resource provided an overview of how HIPAA influences information-sharing between health care providers and food banks and strategies for effective coordination and communication to keep health information safe. In this update, Feeding America and CHLPI highlight additional approaches to sharing information in compliance with HIPAA and respond to questions received (and lessons learned) from food banks that have put the guide into practice.

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.[6] 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.[7] 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?

HISTORY

In 1996, Congress passed HIPAA (shorthand for the "Health Insurance Portability and Accountability Act of 1996") to respond to several developments in the health care sector. Health information was flowing among health care providers, hospitals, and insurers, and across state lines at increasing rates. New health technologies, including the electronic storage of health information, were emerging. Congress stepped in to standardize privacy protections for health information. Since 1996, the federal government has consistently enforced and amended HIPAA, with the goal of better protecting health information in the United States.[8]

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

2000 — **2020**

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.

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 (ePHI) and which gave HHS the authority to make Business Associates of Covered Entities directly liable under HIPAA rules.

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

KEY CONCEPTS

HIPAA is a complicated area of law. The concepts discussed below are intended to help food banks navigate the general structure of obligations in place to protect health information, and introduce common terms likely to come up in early stages of food bank/health care partnership planning. For more information, see *What it Means to Comply with HIPAA* at Appendix E.

Protected Health Information

HIPAA protections apply to a specific subset of information: health information created, used, or maintained by an organization subject to HIPAA requirements in any medium (e.g., on paper, electronically, orally) that can reasonably be tied back to an individual.[9] This information is called Protected Health Information or PHI. HIPAA lists 18 types of information that each comprise PHI when paired with information about an individual's physical or mental health, the provision of health care to an individual, or future payment for the provision of health care to an individual.[10]

The following types of information are considered elements of information that make it identifiable to an individual:

- Names
- Geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, etc.
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web URLs
- IP addresses
- Biometric identifiers, including finger and voice prints
- Photographic images
- Any other unique identifying number, characteristic or code

Covered Entities and Business Associates

Covered Entities and Business Associates are two categories of entities that must comply with HIPAA. Covered Entities under HIPAA are:

1) health plans,
2) health care clearinghouses (entities that process health information), and
3) health care providers that transmit information electronically for certain specified purposes.[11]

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.[12]

Privacy Rule

HIPAA's Privacy Rule in large part defines and limits permitted uses and disclosures—the circumstances in which a Covered Entity (and Business Associates) may use or disclose an individual's PHI. [13]

Security Rule

Electronic PHI (ePHI) is additionally subject to HIPAA's Security Rule. Security Rule standards require administrative, physical, and technical safeguards to ensure the security, confidentiality, and integrity of ePHI.[14]

Minimum Necessary Standard

The Minimum Necessary Standard establishes that Covered Entities (and their Business Associates) must make "reasonable efforts" to ensure that access to PHI is limited to the minimum amount necessary to achieve the purpose of a particular disclosure, request, or use.[15] The Minimum Necessary Standard applies unless otherwise noted in the regulations.[16] This means that even permitted disclosures are generally subject to the requirement.

WHY DO FOOD BANKS NEED TO KNOW ABOUT HIPAA?

A food bank generally does *not* meet the definition of a Covered Entity or Business Associate and is *not* subject to HIPAA based on the provision of food or general nutrition education and related activities. Still, food banks should be knowledgeable about HIPAA for three reasons.

1. Food banks should be familiar with HIPAA because HIPAA is extremely important to their health care partners and collaborators. These requirements can be complicated to navigate and failing to comply with them can have significant negative consequences. Food banks' knowledge about and ability to properly handle patient information (when necessary) will support more effective health care partnerships.

2. As food banks continue to more deeply collaborate with health care, it is possible that they take on new activities that resemble HIPAA's definition 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. *This resource is not written for organizations that are Covered Entities; however, for more information about when food banks might become a Covered Entity, see Appendix D.*

3. Finally, it is important for food banks to understand HIPAA in order to be good self-advocates in forming these new partnerships. Health care partners are often eager to enter into a Business Associate arrangement with food banks, which requires significant investment in compliance with HIPAA and exposes the food bank to compliance risk and, generally, liability.

Being realistic about the new tasks and responsibilities that they are able to incur in the course of partnership will help food banks and their health care partners serve patients and clients without over-stating or over-estimating the food bank's capacity to receive, store, and guard sensitive patient information in a safe and compliant way. It will also help food banks take active steps over time to institute information-holding and sharing methods that are HIPAA-compliant.

HIPAA (and a food bank's ability to navigate HIPAA) may impact the design of the food bank/health care partnership when it comes to whether (and how) PHI is shared.

Photo courtesy of Feeding America.

NAVIGATING HIPAA WHEN SHARING INFORMATION WITH HEALTH CARE PARTNERS

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.[17]

At one end of the spectrum, there are partnerships that do not involve disclosures of PHI from a Covered Entity to a food bank. One version of this partnership is where patients themselves relay their medical information to the food bank. (A patient can always voluntarily disclose any and all of their information.) Another version of this partnership is where the food bank's responsibility is to stock a health care provider's pantry and the food bank only receives de-identified information to enable the activity.

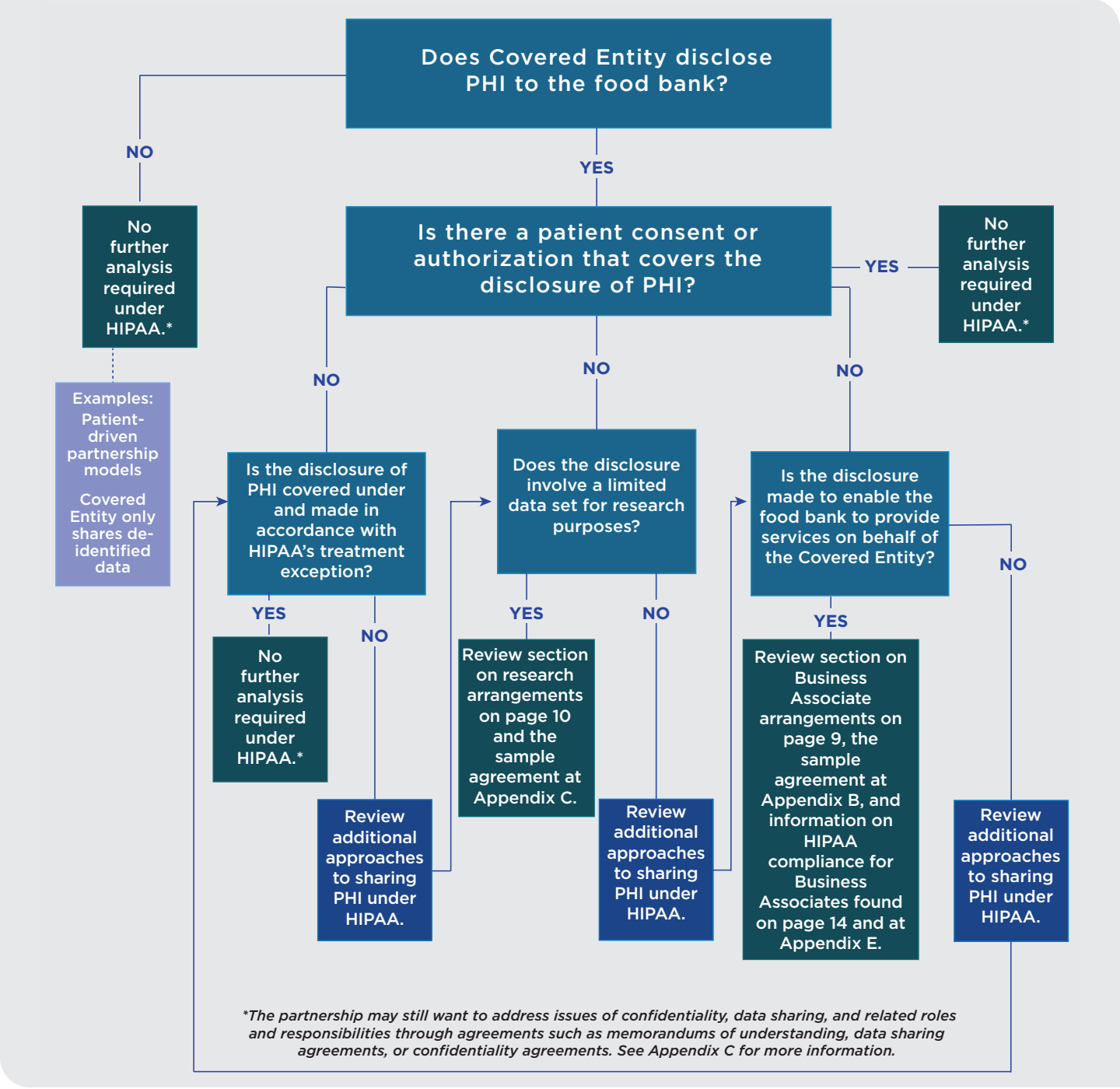
At the other end of the spectrum are partnerships that regularly involve disclosures of PHI, making it necessary to ensure that disclosures are HIPAA-compliant.

Photo courtesy of Feeding America.

APPROACHES TO SHARING PHI UNDER HIPAA: PERMITTED DISCLOSURES

One of the major goals of HIPAA's Privacy Rule is to strike a balance between protecting patient privacy and permitting important uses and disclosures of PHI. This section discusses four different approaches to sharing PHI in a HIPAA-compliant manner that have particular relevance to food bank/health care partnerships:

1) **PATIENT-DRIVEN INFORMATION SHARING BETWEEN FOOD BANKS AND COVERED ENTITIES**
2) **DISCLOSURES FOR TREATMENT PURPOSES**
3) **BUSINESS ASSOCIATE ARRANGEMENTS**
4) **RESEARCH AND PROGRAM EVALUATION ARRANGEMENTS**



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

HIPAA gives patients control of and access to their own PHI. A patient can make a Disclosure Request or complete an Authorization form for a Covered Entity to share information with a food bank. No agreement between the Covered Entity and food bank is required.[18] These are straightforward approaches to sharing information in a manner consistent with HIPAA.

Written Disclosure Requests:

A written Disclosure Request is a request by a patient for the release of PHI to a specified third party. A Covered Entity must comply with any request that is written, signed by the patient, and clearly identifies the intended recipient (and where to send the records), usually within 30 days.[19]

Authorizations:

Authorizations are general releases patients sign that authorize a Covered Entity to share PHI with parties specified in the release.[20] Unlike a written Disclosure Request, an Authorization permits but does not obligate a Covered Entity to share patient information. In order for an Authorization to be valid, it must contain specified elements of information and certain requirement statements.[21]

See a sample Patient Authorization at Appendix A.

Obtaining Authorization

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.

Photo courtesy of Feeding America.

2. DISCLOSURES FOR TREATMENT PURPOSES

A Covered Entity health care provider is permitted to share PHI to advance a patient's treatment.[22] HIPAA defines "treatment" as "the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party."[23] This exception to HIPAA's requirement that PHI be shared through a valid patient authorization is commonly referred to as the "Treatment Exception."

The Treatment Exception

HIPAA allows a Covered Entity health care provider to share PHI in furtherance of a patient's treatment.[24] Under the exception, a health care provider is permitted to share information with a social services organization when the Covered Entity believes that the information may further the individual's health.[25] Patient authorization is not required.

Health plans that are not health care providers do not have the same freedom to share information for treatment purposes.

The Treatment Exception is often used between health care providers. For example, a primary care provider can rely on the Treatment Exception to send PHI to a hospital where her patient is about to have surgery. However, the Treatment Exception can also be used to share PHI between a health care provider and a third party social services organization when the provider believes that disclosure is "a necessary component of, or may help further, the individual's health or mental health care . . . ."[26]

The information shared is subject to the Minimum Necessary Standard.[27] While Covered Entities are ultimately responsible for ensuring their compliance with HIPAA, Covered Entities and food banks can work together to develop standard protocols that address the types and amount of PHI that would be appropriate to disclose to a food bank for purposes of care coordination under the Treatment Exception.

Health care providers may be hesitant to rely on the Treatment Exception in partnerships with food banks. There is not a lot of information available to clarify this application of the Treatment Exception, and the only illustration provided by regulators focuses on housing: Under the Treatment Exception, a health care provider is permitted to share the fact that a specific individual needs mental health care supportive housing with an agency that arranges these services.[28] An analogous illustration *may* be that a health care provider is permitted to share information relating to an individual's nutritional needs with a food bank that arranges for a tailored food box.

3. BUSINESS ASSOCIATE ARRANGEMENTS

A Business Associate is a company or organization that is separate from a Covered Entity but that requires PHI in order to conduct HIPAA-regulated activities on behalf of or provide certain services to a Covered Entity.[29]

There are many ways to structure partnerships between food banks and Covered Entities that do not make the food bank a Business Associate of the Covered Entity. Food banks most commonly find themselves in a Business Associate relationship when the food bank provides "population-based activities relating to improving health or reducing costs" or "case management" for a Covered Entity.[30] A food bank with a contract to provide semi-monthly nutritional advice and coaching to a Covered Entity's patients living with diabetes, for example, may be a Business Associate conducting HIPAA-regulated activities on behalf of the Covered Entity.[31]

Business Associates are responsible for complying with HIPAA requirements, giving rise to liabilities under the law and according to the terms of a "Business Associate Agreement"—an agreement that describes the functions that the Business Associate will carry out for the Covered Entity, and that set forth HIPAA-related rights and responsibilities of the parties. HIPAA mandates that Covered Entities and their Business Associates sign written Business Associate Agreements.

Contracts Caution!

Food banks should carefully consider whether signing a Business Associate Agreement is in their best interest. In lieu of signing a Business Associate Agreement, food banks might explore other options including: (1) encouraging a health care partner to obtain individual patient authorization to disclose PHI; or (2) structuring the partnership in a manner that does not require the health care partner to disclosure PHI.

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.
- Read every part of the Business Associate Agreement carefully. If you do not understand the provisions, ask for clarification. It is important for food banks to understand the extent of the responsibilities and legal obligations they are taking on.
- Conduct a realistic assessment of whether your food bank can meet the additional responsibilities and obligations described in the contract. Also see *What it Means to Comply with HIPAA* at Appendix E. 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.

A food bank that signs a Business Associate Agreement agrees to take on all of the obligations that the Agreement describes and to comply with the applicable requirements of HIPAA. 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 can fulfill the Agreement's obligations. Food banks may also be able to turn to their health care partner for support. Common examples of resources provided by a health care partner include a HIPAA-compliant portal for storing and transmitting information, HIPAA-compliant technology and security support, sample policies and procedures, and HIPAA training/training resources.

See a sample Business Associate Agreement at Appendix B.

4. RESEARCH AND PROGRAM EVALUATION ARRANGEMENTS

Research and evaluation is an important part of many community-clinical partnerships. One approach to sharing information to support these activities involves signing a Data Use Agreement.

A Covered Entity can use a Data Use Agreement to share a "limited data set" with third parties for certain specific, limited purposes, including research.[32] Through a Data Use Agreement, a Covered Entity can share PHI that has been *partially* de-identified. Most identifiers must be removed from the data, but it is permissible for the data set to contain other identifiers that are considered PHI: city, state, and zip code, ages under 90 years, and dates that relate to an individual, such as a birthday or important dates in a medical history. [33]

Important features to note about this approach to sharing PHI include that a Data Use Agreement must: (1) contain certain required content; (2) be in place (signed and effective) before the limited data set is shared; and (3) be study specific.

Similar to Business Associate arrangements, a food bank that signs a Data Use Agreement agrees to take on all of the obligations that the Agreement describes. If a food bank does decide to enter into a Data Use 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. Unlike a Business Associate Agreement, however, a Data Use Agreement does not require the food bank partner to comply with other provisions of HIPAA.

See a sample Data Use Agreement at Appendix C.

Additional Research Arrangements

A Data Use Agreement is not the only way for a food bank to conduct research and evaluation activities. Many food banks in a food bank/health care partnership use de-identified data for these purposes. This information may be received from the health care partner directly, from another institutional partner (such as a university), or from a third party employed to de-identify the data.

Depending on the substance of the research project, approval may be required from an Institutional Review Board—a committee or other group formally designated by an institution to review research involving human subjects. Institutional Review Boards are also able to waive restrictions on the sharing of PHI for research purposes (e.g., that disclosures are subject to a valid authorization or that only a limited data set may be shared) if it determines that certain criteria are satisfied, including that there is an adequate plan in place to protect PHI from improper use and disclosure, and that the research could not practicably be conducted without both the data and the waiver.[34]

Photo courtesy of Feeding America.

PARTNERSHIP EXAMPLES

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 the information received...		Comments and Considerations
	specific to an individual?	from a Covered Entity or Business Associate?	
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 them to the food bank representative and is present during the introduction. The patient shares information 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. • Care should be taken not to give the impression that the food bank is collecting information for the health care partner. Alternatively, the food bank may want to secure patient consent to share information back with the health care partner to facilitate, for example, research and evaluation.
Covered Entity facilitates enrollment into program operated by food bank. 1. The Covered Entity identifies a patient as food insecure. 2. The Covered Entity provides patient with a paper or electronic application to a program operated by the food bank. 3. The patient submits an application to the food bank.	Yes	No	• This scenario is similar to the scenario above. The patient ultimately shares information with the food bank directly.

Scenario	Is the information received...		Comments and Considerations
	specific to an individual?	from a Covered Entity or Business Associate?	
The Covered Entity provider gives the patient information about the type of food box they 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 banks 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 bank and explains their diagnosis or their diagnosis-related needs for their 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 their information. • Care should be taken not to give the impression that the food bank is collecting information for the health care partner. Alternatively, the food bank may want to secure patient consent to share information back with the health care partner to facilitate, for example, research and evaluation. **Limitations** • The food bank will not be able to conduct initial 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 sites.
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 food bank location the food boxes should be distributed. 2. The food bank prepares the food boxes and has them ready at the applicable food bank locations. 3. Patients present at the food bank location and request the applicable food box.	No	Yes	• The Covered Entity does not share any individually identifiable health information. • The Covered Entity may be concerned about incidental exposure to PHI when, for example, food bank representatives are dropping off food boxes at the food bank. Generally, a simple confidentiality provision is sufficient to address the Covered Entity's concerns in this scenario. **Limitations** • 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 food bank location 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.

Scenario	Is the information received...		Comments and Considerations
	specific to an individual?	from a Covered Entity or Business Associate?	
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 their health information as long as it is in writing, is signed by the patient, and clearly specifies the intended recipient of the information.[35] **Hybrid Approach** • Some partnerships have taken a hybrid approach in which the Covered Entity sends very basic information (i.e., patient name and contact information) to the food bank after securing patient consent or authorization. From there, the food bank conducts outreach and gets any additional information (e.g., health information) from the patient directly.
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 HIPAA and the terms of the Business Associate Agreement. Compliance may 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.

HIPAA COMPLIANCE: IS THERE AN APP FOR THAT?

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. Food banks that seek to become HIPAA compliant should be prepared to invest time and resources in order to do the following:

1) **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.[36]

2) **Train staff**

   Food banks must develop training materials that inform *all* workforce members about HIPAA and relevant HIPAA-related policies and procedures.

3) **Implement safeguards to protect PHI**

   Food banks that seek to become HIPAA compliant should assess risks and vulnerabilities with respect to how PHI is created, transmitted, and/or received, and they may need to invest in equipment, technology, software, new locks, and other measures to be sure they are following HIPAA rules and any additional requirements they may have agreed to in a Business Associate Agreement.

Food banks exploring HIPAA may hear about "HIPAA-compliant software" and "HIPAA compliance software." The term HIPAA-compliant software is used to refer to software that has incorporated HIPAA security safeguards into the way information is stored, retrieved, and transmitted (e.g., unique user identifications to support authentication that someone accessing PHI is who they say they are, e-mail encryption to ensure the secure transmission of ePHI). HIPAA compliance software refers to software products that offer different tools to manage HIPAA requirements (e.g., customizable policies and procedures, training materials).

Focusing on HIPAA-compliant software, the following points should be kept in mind by food banks exploring this kind of product:

HIPAA does not require that organizations invest in any particular technology solution(s).[37] Not every organization has the capacity to use complex or expensive technology platforms to handle PHI, and a food bank must decide what security strategies will be most effective *and* most realistic to adopt. Additional guidance on making these kinds of determinations is provided in "Four Steps to Developing a Security Management Plan for Business Associates > Step 2: Develop an Action Plan to Protect PHI and Mitigate Risk" on page 31.

Use of HIPAA-compliant software does not itself achieve compliance. Organizations are still responsible for carrying out their compliance program, and for ensuring that the way they use any software comports with HIPAA.

There is no official certification program. When a company markets a product as HIPAA compliant, it is making a claim (typically based on the fact that the product was development to meet HIPAA requirements specifically). The safeguards outlined on page 34 can be used as a checklist to help evaluate the quality of a particular product.

Many of the popular suppliers of organizational software packages/products, including Microsoft,[38] Google,[39] Slack,[40] and Zoom,[41] have specific products that they identify as HIPAA compliant, and publish guidance on specific steps organizations must take in order to configure software for HIPAA compliance. Food banks *should not* assume that any given product by one of these companies is HIPAA compliant.

Oftentimes, Covered Entities and Business Associates must sign a Business Associate Agreement with the software vendor.[42] If the company is experienced in working with organizations subject to HIPAA, it will be familiar with this requirement and likely have a template agreement that they use with customers.

Increasingly, health care providers are using community resource referral platforms to facilitate partnerships with food banks and other community-based organizations. While the full range of functionality differs across products, many include basic information sharing capabilities

and secure messaging options to support care coordination. In 2019, the Social Interventions Research and Evaluation Network (SIREN) published a detailed review of nine products, which includes information on HIPAA compliance, functionalities, and even opportunities for health care organizations to secure funding for community resource referral platforms. (Visit https://sirenetwork.ucsf.edu/ for more information and to access the resource, *Community Resource Referral Platforms: A Guide for Health Care Organizations.*)

See Appendix E for more on HIPAA compliance.

Photo courtesy of Feeding America.

CONCLUSION

Forging successful food bank/health care 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.

As partners align on program design and their preferred approach(es) to sharing information in a manner that is compliant with HIPAA, the materials in the appendices that follow—including template agreements and more information on what it means to comply with HIPAA—can support food banks in taking the next steps.

Together, food banks and their health care partners can promote the health and well-being of the populations they serve.

APPENDIX A: TEMPLATE PATIENT AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

A valid written authorization must include:

(1) a specific and meaningful description of the information to be shared,
(2) a description of each purpose of the disclosure,
(3) an identification of the person or entity authorized to make the disclosure,
(4) an identification of the recipient(s) of the information,
(5) an expiration date or event for the authorization, and
(6) the patient's signature and the date.[43]

The authorization also must inform the patient of:

(1) their 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.[44]

Finally, the authorization must be written in plain language, and the Covered Entity must give a copy of the authorization to the patient.[45] State laws and regulations may impose additional requirements or restrictions on written authorizations.[46]

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).

HIPAA allows a single authorization to state that a broad class of persons, e.g., "social service providers," is able to receive/use PHI.[47] Descriptions of the information released ("3. Extent of Authorization") and the purpose of the disclosure ("4. Use of Disclosure") should be revised to reflect a broader range of supportive activities. This approach may appeal to health care partners interested in administrative simplification.

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
- ☐ Genetic (inherited) diseases or tests
- ☐ Other (please specify): _____

In general, food banks may want to avoid having access to more sensitive information such as information pertaining to mental health records, communicable diseases, genetic information, and treatment for alcohol or drug abuse. One option to limit access is to explicitly state that these categories of information are not included in the authorization.

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.

When a Covered Entity receives an authorization to disclose PHI, disclosures must be consistent with that authorization. Partnerships should ensure that this section accurately describes how food banks are using PHI, especially if activities evolve over time. For example, if one purpose of the disclosure is for food banks to conduct research on the effectiveness of the partnership, this section should identify that purpose.

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 B: 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 imposes legal obligations, including to comply with 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

This Business Associate Agreement applies to the parties only to the extent that a business associate relationship exists within the meaning of 45 CFR 160.103.

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 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 to Appendix E, 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;

It is common for a Covered Entity to include a reporting requirement for suspected breaches or security incidents. This is not, however, required under HIPAA.

It is also common for a Covered Entity to include a 10-, 15-, or 30-day timeframe for reporting. This is not required under HIPAA, however, Covered Entities must notify the Secretary of Health and Human Services within 60 days of an incident and state law may impose more stringent requirements. Food banks should be aware of variations across their Agreements.

(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). 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).

Obligations of Covered Entity

(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 their 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 regarding Covered Entity's privacy practices and restrictions that may be relevant to the food bank's policies and procedures.

(d) *[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.

(e) *[Optional]* When Covered Entity discloses protected health information to Business Associate, Covered Entity shall provide no more than the minimum amount necessary for Business Associate to accomplish its purpose.

While these are optional clauses in a Business Associate Agreement, they obligate the Covered Entity to take certain steps to support food bank's compliance with HIPAA and the Agreement. The Agreement could go so far as to specify the information that is needed in order for the food bank to carry out its functions and, therefore, the types of information to which the food bank will have access.

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.

Indemnification and Liability Clauses

Indemnification provisions typically indicate that the Business Associate will assume all civil liability for an unauthorized use or disclosure of PHI. This type of provision is not required under HIPAA and food banks should be very cautious about agreeing to indemnification as it could leave them bearing costly and unanticipated monetary responsibility for a violation of the agreement or HIPAA rules. In the event that a health care partner is insisting on indemnification, food banks can attempt to negotiate limits such as:

- *Business Associate's total liability relating to this Agreement shall not exceed _____ [Insert amount].*
- *The parties agree that expenses of not more than _____ [Insert amount] per affected individual are reasonable expenses subject to indemnification if incurred in response to a security incident.*
- *Business Associate shall not be liable to Covered Entity for any special, consequential, incidental, or exemplary damages.*
- *Business Associate shall not be liable for damages caused by Covered Entity's negligence or willful misconduct.*

Signatures

Name: _____ (Food Bank Representative)
Signature: _____ (Food Bank Representative)

Name: _____ (Covered Entity Representative)
Signature: _____ (Covered Entity Representative)

APPENDIX C: TEMPLATE DATA USE AGREEMENT

This template agreement is based on standards specified under HIPAA.[48] Each section is a required section; 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.

DATA USE AGREEMENT BETWEEN [HEALTH CARE ENTITY] AND [FOOD BANK]

This Data Use Agreement, effective as of _____, _____, is entered into by and between [Food Bank] ("LDS Recipient") and [Health Care Entity] ("Covered Entity"). The purpose of this Agreement is to provide Recipient with access to a Limited Data Set ("LDS Information") for use in the following research project in accordance with HIPAA: [Parties should insert here the name of the research project (if any) and a short description].

1. Preparation of LDS Information. Covered Entity shall prepare and furnish to LDS Recipient the LDS Information in accordance with HIPAA.
2. Permitted Uses and Disclosures. LDS Recipient may use LDS Information to conduct the research described in this Data Use Agreement.
3. Prohibitions on Use and Disclosure. LDS Recipient is prohibited from using or further disclosing LDS Information, except as permitted by the agreement or as permitted by law. LDS Recipient shall not use LDS Information to identify and/or contact individuals to whom the LDS Information relates.
4. Safeguards. LDS Recipient shall use appropriate safeguards to prevent a use or disclosure of LDS Information that is not permitted by this Data Use Agreement.
5. Reporting of Disclosures. LDS Recipient shall notify Covered Entity in writing within [___] working days of its discovery of any unauthorized use or disclosure of the LDS Information of which LDS Recipient becomes aware.
6. Restrictions on Agents. LDS Recipient shall ensure that any agents, including a subcontractor, to whom LDS Recipient provides LDS Information will agree to the same restrictions as set forth in this Data Use Agreement.

Signatures

Name: _____ (Food Bank Representative)
Signature: _____ (Food Bank Representative)

Name: _____ (Covered Entity Representative)
Signature: _____ (Covered Entity Representative)

The elements of a Data Use Agreement are governed by HIPAA. Food bank/health care partnerships that are not subject to this particular requirement may want to enter into agreements that establish parameters to how the parties use and protect information. The provisions above can be used to develop memorandums of understanding, confidentiality agreements, non-disclosure agreements, and other forms of data sharing agreements.

Food banks should ensure that their own information and interests are protected through provisions that address, for example:

- *ownership of food bank's data and of any work product resulting from food bank's services under the agreement;*
- *whether the health care partner has an interest in or rights to the use of food bank's data for a purpose other than performance of the health care partner's obligations under the agreement; and*
- *reasonable safeguards to protect confidential information provided to the health care partner by the food bank.*

APPENDIX D: WHEN MIGHT A FOOD BANK BE CONSIDERED A COVERED ENTITY?

Only certain entities are HIPAA-Covered Entities: (1) health plans, (2) health care clearinghouses, and (3) health care providers that electronically transmit health information in connection with a covered transaction.[49] Therefore, 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 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; (2) provide medical or health services;[50] or (3) furnish, bill, or are paid for health care in the normal course of business are health care providers under HIPAA.[51]

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.[52]

Food banks are *not* a "provider of services" under this definition.[53]

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[54] 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.[55] 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 electronically 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.[56]

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.[57] 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."[58] 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."[59] A food bank that regularly fills "prescriptions" for food boxes could potentially be considered a health care provider under HIPAA based on a broad reading of the definitions above. On the other hand, the U.S. Department of Health and Human Services generally classifies the provision of food/produce as a non-primarily health related support, which suggests that food banks filling "prescriptions" for food boxes should not be considered a health care provider.[60]

Food banks should consult with an attorney before using the term "prescription" in the context of food bank 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.[61] 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.[62] 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.[63]

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.

As above, conducting a covered transaction electronically is not enough to qualify the food bank as a Covered Entity if the food bank is not also a health care provider under HIPAA. While a food bank may, for example, transmit information electronically to a health plan in connection with payment for services provided to a health plan's members, this alone does not cause the food bank to meet the definition of a Covered Entity.

Examples

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 bank 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 bank.
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 them 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. 25, 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.[64]
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 bank regularly fills patients' "prescriptions" from a clinic for food boxes.	Yes	No	Since the food bank technically fills prescriptions in the normal course of business, it may meet HIPAA's broadly worded definition of a health care provider.[65] However, the provision of food/produce is generally characterized as a non-primarily health related support, which supports the argument that food banks using the term "prescription" to distribute food are not health care providers. Regardless, because there is no electronic transmission in connection with a covered transaction, the food bank is therefore not a Covered Entity. It may be advisable to use a term other than "prescription" (e.g., voucher, food package) in these programs.
A food bank 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 bank 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 food box the patient needs and has an identifying number for the patient. The food bank then emails the clinic the numbers on the forms the patients provided.	No	No	This operation does not make the food bank a health care provider under HIPAA. By giving the form to the food bank, the patient has chosen to disclose information about their health status. The patient always has the right to disclose their PHI to any third party they 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.

APPENDIX E: WHAT IT MEANS TO COMPLY WITH HIPAA

As a general matter, Covered Entities must ensure compliance with the HIPAA Security, Breach Notification, and Privacy Rules; food banks that are Business Associates must comply with the HIPAA Security Rule and Breach Notification Rule as well as certain provisions of the HIPAA Privacy Rule.[66] This Appendix will provide an overview of obligations under these different categories that are relevant to food banks.

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.[67]

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[68] 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;
- protect against reasonably anticipated, impermissible uses or disclosures; and
- ensure compliance by their workforce.[69]

The Security Rule also asks Covered Entities and their Business Associates to put in place specific safeguards. These safeguards, organized into administrative, physical, technical, organizational, and documentation requirements, should inform the development of an organization's compliance program.

☑ 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.[70] 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;[71] implementing appropriate security measures to address the risks identified in the risk analysis, like encrypting information;[72] documenting what security measures are chosen and the rationale for adopting those measures;[73] and ensuring that security protections are maintained.[74] HHS encourages organizations to make risk analysis an ongoing, iterative process.[75]

☐ **Security Personnel**
A Covered Entity or Business Associate must designate a security official responsible for developing and implementing security policies and procedures. [76]

☐ **Information Access Management**
A Covered Entity or Business Associate must implement policies and procedures for "minimum necessary" role-based access.[77]

☐ **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.[78] It must also have sanctions in place for individuals that violate them.[79]

☐ **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.[80]

☑ Physical Safeguards

☐ **Facility Access and Control**
A Covered Entity or Business Associate must limit unauthorized, physical access to its facilities.[81]

☐ **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.[82]

☑ Technical Safeguards

☐ **Access Control**
A Covered Entity or Business Associate must implement technical policies and procedures that allow only authorized access to electronic PHI.[83]

☐ **Audit Controls**
A Covered Entity or Business Associate must put in place mechanisms to record and examine information systems that contain or use electronic PHI.[84]

☐ **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. [85]

☐ **Person or Entity Authentication**
A Covered Entity or Business Associate must put in place mechanisms to verify that a person or entity seeking access to electronic protected health information is the one claimed.[86]

☐ **Transmission Security**
A Covered Entity or Business Associate must prevent unauthorized access to PHI transmitted over a network.[87]

☑ Organizational, 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:[88]

- 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.[89]

☐ **Updates**
A Covered Entity or Business Associate must periodically review and update documentation as changes that affect the security of electronic PHI occur.[90]

☐ **Organizational Standards**
The focus of organizational standards is requirements for business associate agreements and certain other arrangements. Note that if a Business Associate has subcontractors that handle or access PHI on their behalf, the Business Associate is generally required to enter into Business Associate Agreements with those subcontractors.

Spotlight on the Security Management Process: Four Steps to Developing a Security Management Plan for Business Associates

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.[91] 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. *The overview below is adapted from the ONC's "Sample Seven-Step Approach for Implementing a Security Management Process."* [92] *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 makes the following resources available:

- Regional Extension Centers assistance[93]
- Office of the National Coordinator for Health Information Technology (ONC) Health IT Privacy and Security Resources web page[94]
- Office for Civil Rights Security Rule Guidance Material[95]
- Office for Civil Rights audit protocols[96]

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.[97] 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.[98] 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**.

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.[99] 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:[100]

- 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,[101] physical safeguards,[102] technical safeguards,[103] organizational standards,[104] and policies and procedures.[105] 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.

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. Not every organization has 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:[106]

- the size, complexity, and capabilities of your organization;
- the technical infrastructure, hardware, and software security capabilities of your organization;

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.

- 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,[107] a food bank might improve its physical safeguards 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[108]

- 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[109]

Written policies and procedures should, at a minimum:

- Establish protocols for all five security components listed in in the table on page 32.
- 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.

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.[110] 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.

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.[111]
- Consistently apply your policies and procedures when unauthorized access to PHI occurs.[112]
- Periodically review your policies and procedures to make sure they are current and your practice adheres to them.[113]
- 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).[114]

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 strategies 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,[115] 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.[116] Audit control and capabilities should again be scaled to the size of the organization.

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. [117]

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.[118] Two types of PHI are relevant here:[119]

- Secured PHI: An unauthorized person cannot access, 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 access, use, read, and decipher PHI that this person obtains because your organization does not appropriately safeguard, encrypt, or destroy the PHI; or encrypts PHI, but the decryption key has also been breached.

Breach Risk Assessment. 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:[120]

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.[121]

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[122] 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[123] of the breach.[124] 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:[125]

—*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 single 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.

State laws and the terms of a Business Associate Agreement regarding data breach notification may create different/additional obligations. For example, certain breaches may trigger a requirement to notify a state agency. Food banks should also review these resources when designing related policies and procedures.

Requirements for Business Associates Under Privacy Rule

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

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.[127] The contours of this are dictated by 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 *See, e.g.,* Dietary Guidelines Advisory Comm., *Scientific Report of the 2015 Dietary Guidelines Advisory Committee: Advisory Report to the Secretary of Health and Human Services and the Secretary of Agriculture* (2015), https://health.gov/sites/default/files/2019-09/Scientific-Report-of-the-2015-Dietary-Guidelines-Advisory-Committee.pdf.

3 *See Social Determinants of Health: Know What Affects Health,* Ctrs. for Disease Control & Prevention, https://www.cdc.gov/socialdeterminants/index.htm (last visited Feb. 6, 2020).

4 These regulations are the Privacy Rule, the Security Rule, the Enforcement Rule, and the Final Omnibus Rule. *See* U.S. Dep't of Health & Human Servs., *HIPAA for Professionals*, HHS.gov, http://www.hhs.gov/hipaa/for-professionals/index.html (last visited Feb. 6, 2020).

5 U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Privacy Rule* 1 (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

6 *See* Off. of Nat'l Coordinator for Health Info. Tech., *HIPAA versus State Laws,* HealthIT.gov, https://www.healthit.gov/topic/hipaa-versus-state-laws (last visited May 20, 2020).

7 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.

8 U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Privacy Rule* 1 (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

9 45 C.F.R. § 160.103.

10 45 C.F.R. § 160.103; 45 C.F.R. § 164.514(b)(2)(i).

11 45 C.F.R. § 160.103.

12 45 C.F.R. § 160.103.

13 45 C.F.R. §§ 160, 164(A), 164(E).

14 45 C.F.R. §§ 164.302-164.318.

15 45 C.F.R. § 164.502(b).

16 45 C.F.R. § 164.502(b).

17 *See* 45 C.F.R. § 160.103.

18 *See* 45 C.F.R. § 164.502; 45 C.F.R. § 164.524.

19 *See* 45 C.F.R. § 164.524.

20 *See* 45 C.F.R. § 164.502(a)(1)(iv).

21 45 C.F.R. § 164.508.

22 45 C.F.R. § 164.506.

23 45 C.F.R. § 164.501.

24 45 C.F.R. § 164.506(b)(1).

25 U.S. Dep't of Health & Human Servs., *FAQ 3008: Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-Hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html (last visited Sept. 16, 2019).

26 U.S. Dep't of Health & Human Servs., *FAQ 3008: Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-Hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html (last visited Sept. 16, 2019).

27 U.S. Dep't of Health & Human Servs., *FAQ 3008: Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-Hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html (last visited Sept. 16, 2019).

28 U.S. Dep't of Health & Human Servs., *FAQ 3008: Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-Hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html (last visited Sept. 16, 2019).

29 45 C.F.R. § 160.103.

30 *See* U.S. Dep't of Health and Human Servs. et al., Permitted Uses and Disclosures: Exchange for Health Care Operations (2016), https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf.

31 *See* U.S. Dep't of Health and Human Servs. et al., Permitted Uses and Disclosures: Exchange for Health Care Operations (2016), https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf (providing illustration of the exchange of PHI for case management and population-based activities in which HHS identifies that a health care management company providing semi-monthly nutritional advice and coaching to a health plan's members is a Business Associate of the health plan).

32 *See* 45 C.F.R. § 164.514(e). Under HIPAA, research is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 42 C.F.R. § 164.501. Other permitted purposes for a Data Use Agreement are public health and health care operations. 45 C.F.R. § 164.514(e).

33 *See* 45 C.F.R. § 164.514(e)

34 *See* 45 C.F.R. § 164.512(i). Factors for consideration by an Institutional Review Board in determining whether a waiver for research purposes would be appropriate are: the presence of an adequate plan to protect identifiers from improper use and disclosure; the presence of an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research; adequate written assurances that, subject to certain exceptions, the PHI will not be reused or redisclosed; whether the research could practicably be conducted without the waiver; and whether the research could practicably be conducted without access to the information. 45 C.F.R. § 164.512(i).

35 *See* 45 C.F.R. § 164.524.

36 *See* 45 C.F.R. § 164.316. *See also* 45 C.F.R. § 164.306(d).

37 *See* U.S. Dep't of Health & Human Servs., *FAQ 2001: Do the standards of the Security Rule require use of specific technologies?*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/faq/2011/do-the-standards-of-the-security-rule-require-use-of-specific-technologies/index.html (last visited Sept. 16, 2019).

38 *See* Microsoft, Health Insurance Portability and Accountability (HIPAA) & HITECH Acts (2020), https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-hipaa-hitech.

39 *See* Google, G Suite and Cloud Identity: HIPAA Implementation Guide (2019), https://static.googleusercontent.com/media/gsuite.google.com/en//terms/2015/1/hipaa_implementation_guide.pdf.

40 *Slack and HIPAA*, Slack, https://slack.com/help/articles/360020685594-Slack-and-HIPAA (last visited Dec. 28, 2019).

41 *Zoom for Health Care*, Zoom, https://zoom.us/healthcare (last visited Dec. 28, 2019).

42 *See* U.S. Dep't of Health &Human Servs., *Guidance on HIPAA & Cloud Computing*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html (last visited Dec. 28, 2019).

43 *See* 45 C.F.R. § 164.508(c). 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).

44 45 C.F.R. § 164.508(c)(2).

45 45 C.F.R. § 164.508(c)(3)-(4).

46 *See, e.g.*, U.S. Dep't of Health & Human Servs., *FAQ 476: Must an authorization include an expiration date?*, HHS.gov, 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").

47 *See* U.S. Dep't of Health & Human Servs., *FAQ 3008: Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-Hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html (last visited Sept. 16, 2019).

48 *See* 45 C.F.R. § 164.514(e).

49 45 C.F.R. § 160.103.

50 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).

51 45 C.F.R. § 160.103.

[52] *See* 45 C.F.R. § 160.103 (referring to 42 U.S.C.A. § 1395x(u) in the definition of "health care provider").
[53] *See* 45 C.F.R. § 160.103 (referring to 42 U.S.C.A. § 1395x(u) in the definition of "health care provider").
[54] *See* 45 C.F.R. § 160.103 (including volunteers in the definition of "workforce").
[55] 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).
[56] 45 C.F.R. § 160.103.
[57] *See* 45 C.F.R. § 160.103.
[58] 45 C.F.R. § 160.103.
[59] 45 C.F.R. § 160.103.
[60] *See, e.g.*, Memo from U.S. Dep't of Health & Human Serv. to Medicare Advantage Organizations on Supplemental Benefits for Chronically Ill Enrollees (Apr. 24, 2019)..
[61] 45 C.F.R. § 160.103.
[62] *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).
[63] 45 C.F.R. § 160.103.
[64] *See* 45 C.F.R. § 160.103; Ctrs. for Medicare & Medicaid Servs., *Referral Certification and Authorization*, CMS.GOV, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/ReferralCertificationandAuthorization (last visited Feb. 6, 2020).
[65] *See* 45 C.F.R. § 160.103.
[66] *See generally* 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e).
[67] *See* U.S. Dep't of Health & Human Servs., *Summary of the HIPAA Security Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Feb. 26, 2017).
[68] 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.
[69] *See* 45 C.F.R. § 164.306(a).
[70] *See* 45 C.F.R. § 164.306(b)(2).
[71] *See* 45 C.F.R. § 164.306(b)(iv).
[72] *See* 45 C.F.R. § 164.308(a)(1)(ii)(B).
[73] *See* 45 C.F.R. § 164.306(d)(3)(ii)(B); 45 C.F.R. § 164.316.
[74] *See* 45 C.F.R. § 164.306(e).
[75] *See* 45 C.F.R. § 164.306; 45 C.F.R. § 164.308.
[76] *See* 45 C.F.R. § 164.308(a)(2).
[77] *See* 45 C.F.R. § 164.308(a)(4).
[78] *See* 45 C.F.R. § 164.308(a)(5).
[79] *See* 45 C.F.R. § 164.308(a)(ii)(C).
[80] *See* 45 C.F.R. § 164.308(a)(8).
[81] *See* 45 C.F.R. § 164.310(a).
[82] *See* 45 C.F.R. §§ 164.310(b)-(d).
[83] *See* 45 C.F.R. § 164.312(a).
[84] *See* 45 C.F.R. § 164.312(b).
[85] *See* 45 C.F.R. § 164.312(c).
[86] *See* 45 C.F.R. § 164.312(d).
[87] *See* 45 C.F.R. § 164.312(e).
[88] *See* 45 C.F.R. § 164.306(b)(2).
[89] *See* 45 C.F.R. § 164.316.
[90] *See* 45 C.F.R. § 164.316(b)(2)(iii).
[91] *See generally* OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf..
[92] OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION 35 (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[93] *See* Off. of Nat'l Coordinator for Health Info. Tech., *Regional Extension Centers*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/regional-extension-centers-recs (last visited Feb. 26, 2017).
[94] *See* Off. of Nat'l Coordinator for Health Info. Tech., *Health IT Privacy & Security Resources*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources (last visited Feb. 26, 2017).
[95] *See* U.S. Dep't of Health & Human Servs., *Security Rule Guidance Material*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index. html (last visited Feb. 26, 2017).
[96] *See* U.S. Dep't of Health & Human Servs., *Audit Protocol*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/ index.html (last visited Feb. 26, 2017).
[97] *See* Off. of Nat'l Coordinator for Health Info. Tech., *Health IT Privacy & Security Resources*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources (last visited Feb. 26, 2017).
[98] *See* Off. of Nat'l Coordinator for Health Info. Tech., *Security Risk Assessment Tool*, HEALTHIT.GOV, https://www.healthit.gov/providers-professionals/security-risk-assessment-tool (last visited Feb. 26, 2017).
[99] *See* 45 C.F.R. § 164.316.
[100] *See* OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION 40 (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[101] *See* 45 C.F.R. § 164.308.
[102] *See* 45 C.F.R. § 164.310.
[103] *See* 45 C.F.R. § 164.312.
[104] *See* 45 C.F.R. § 164.314.
[105] *See* 45 C.F.R. § 164.316.
[106] *See* 45 C.F.R. § 164.306(b)(2)
[107] *See* 45 C.F.R. § 164.310(c).
[108] OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION 44 (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[109] OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION 48 (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[110] *See* 45 C.F.R. § 164.308(a)(5)(i).
[111] *See* 45 C.F.R. § 164.308(a)(5)(i).
[112] *See e.g.*, 45 C.F.R. § 164.308(a)(1)(ii)(C).
[113] *See* 45 C.F.R. § 164.316(b)(2)(iii).
[114] *See* 45 C.F.R. § 164.316(b)(2)(i).
[115] *See* 45 C.F.R. § 164.316(b)(2)(iii).
[116] *See* 45 C.F.R. § 164.312(b).
[117] *See generally* U.S. Dep't of Health & Human Servs., *Submitting Notice of a Breach to the Secretary*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017); U.S. Dep't of Health & Human Servs., *Breach Notification Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited May 20, 2020); OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION 56 (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[118] *See* 45 C.F.R. § 164.402.
[119] OFF. OF NAT'L COORDINATOR FOR HEALTH INFO. TECH., GUIDE TO PRIVACY & SECURITY OF ELECTRONIC HEALTH INFORMATION 58 (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
[120] *See* 45 C.F.R. § 164.402(2).
[121] *See* 45 C.F.R. § 164.402(1) ("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.").
[122] *See* U.S. Dep't of Health & Human Servs., *Submitting Notice of a Breach to the Secretary*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).
[123] *See* 45 C.F.R.§164.404; U.S. Dep't of Health & Human Servs., *Breach Notification Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited May 20, 2020). Per regulation, "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." 45 C.F.R. § 164.404(a)(2).
[124] *See* U.S. Dep't of Health & Human Servs., *Submitting Notice of a Breach to the Secretary*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).
[125] *See* U.S. Dep't of Health & Human Servs., *Submitting Notice of a Breach to the Secretary*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 26, 2017).
[126] *See generally* U.S. Dep't of Health & Human Servs., *Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last visited May 20, 2020).
[127] *See* 45 C.F.R. § 164.504(e)(2)(ii)(H).

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

Health Law Lab
CENTER FOR HEALTH LAW AND POLICY INNOVATION
HARVARD LAW SCHOOL

FEEDING AMERICA