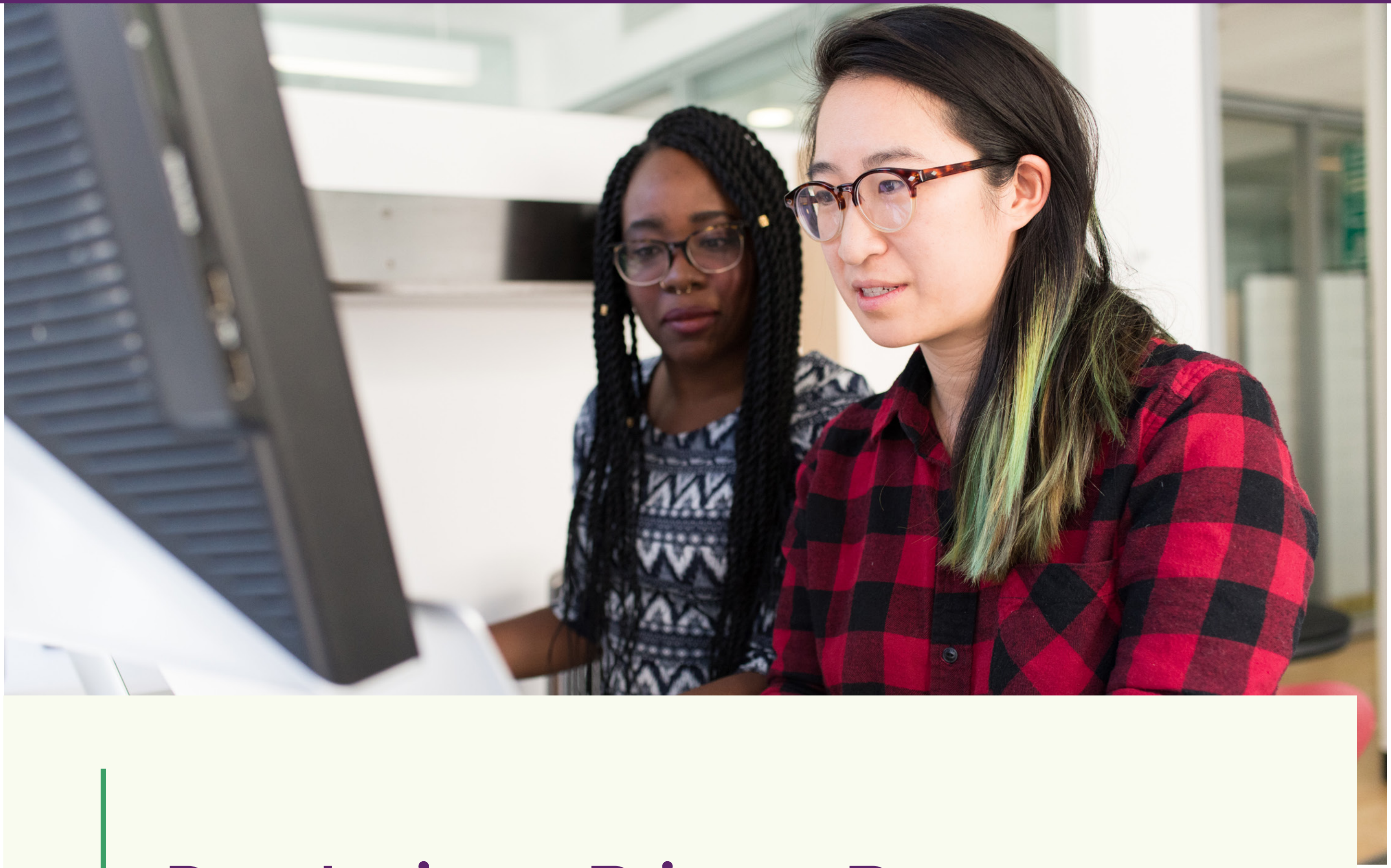
Nutrition Incentive Hub
CREATED BY GUSNIP NTAE CENTER



Developing a Privacy Program

HIPAA Issue Brief 5 of 5

Resource Created by: Center for Health Law and Policy Innovation of Harvard Law School

January 2022

This work is supported by Gus Schumacher Nutrition Incentive Program grant no. 2019-70030-30415/project accession no. 1020863 from the USDA National Institute of Food and Agriculture.

About this Brief and the Series

This resource was created for the GusNIP Nutrition Incentive Program Training, Technical Assistance, Evaluation, and Information Center (NTAE) by the Center for Health Law and Policy Innovation of Harvard Law School. It is part of a series of briefs intended to educate GusNIP Produce Prescription grantees on patient privacy laws; these briefs should not be considered legal advice. For specific legal questions, consult an attorney.

This fifth brief of the series reviews key considerations for developing a privacy program.

The other briefs in this series cover the following foundational HIPAA compliance topics relevant to Produce Prescription grantees:

- **Introduction to Patient Privacy Laws for Produce Prescription Grantees (Issue Brief 1)**
  This brief discusses patient privacy laws for Produce Prescription grantees.
- **Developing HIPAA-Compliant Approaches to Information Sharing (Issue Brief 2)**
  This brief discusses different approaches to structuring the collection and dissemination of participant information in a manner compliant with HIPAA.
- **HIPAA, Program Evaluation, and Research (Issue Brief 3)**
  This brief discusses approaches to navigating HIPAA for programmatic evaluation and research.
- **Business Associate Arrangements (Issue Brief 4)**
  This brief provides additional information on Business Associates and Business Associate Arrangements—a common but resource intensive approach to structuring information sharing from health care providers to third parties.

This brief discusses key components of a HIPAA compliance program, a topic of particular interest to GusNIP Produce Prescription grantees that sign Business Associate Agreements (BAAs) and other grantees that are looking to become compliant with HIPAA. This brief also discusses best practices for the development of a *voluntary* privacy program.

> **Why voluntarily adopt a privacy program?**
> For many grantees, the structure of their activities may not subject them to any obligations under HIPAA. Even so, integrating protections to support the privacy and security of participant information is a good organizational practice—one that is important to building and maintaining participant trust, respecting participant autonomy, and ensuring high-quality data. For more information, see "Guiding Principles for the Voluntary Adoption of a Privacy Program," later in this document.

Grantees share data with the GusNIP NTAE to contribute to an aggregated dataset that will help to understand GusNIP's aggregate impact. Grantees should take every effort to de identify data that is shared with the GusNIP NTAE.

Developing a HIPAA Compliance Program

GusNIP Produce Prescription grantees that seek to develop a HIPAA-compliant privacy program should be prepared to invest time and resources in the following:

(1) Developing and documenting policies

One of the most important aspects of ensuring HIPAA compliance is developing and documenting policies and procedures that organizations adopt to protect Protected Health Information (PHI).

> **Policies and Procedures**
> HIPAA requires that specific policies and procedures be put in place covering, for example, permitted, required, and prohibited uses and disclosures of PHI; the minimum necessary standard; patient rights; procedures for onboarding and working with business associates and business associate subcontractors; notification requirements in the event of a breach; and other administrative requirements, such as appointing a Privacy Officer, investigating inappropriate uses and disclosures of PHI, sanctions against workforce members for violations of policies, etc.

(2) Training

Organizations must train all workforce members about HIPAA and relevant HIPAA-related policies and procedures. While trainings should ultimately be tailored to address an organization's specific policies and procedures, the federal government has developed a series of HIPAA training resources that may be helpful. (Visit https://www.hhs.gov/hipaa/for-professionals/training/index.html to access training materials.)

(3) Implementing safeguards to protect PHI

HIPAA's Security Rule requires organizations to put in place several administrative, technical, and physical safeguards to protect PHI. Organizations that seek to become HIPAA compliant must assess risks and vulnerabilities with respect to how PHI is created, transmitted, and/or received, and organizations may need to invest in equipment, technology, software, new locks, and employ other measures to ensure they are monitoring their organization's activities and following HIPAA rules.

Guiding Principles for the Voluntary Adoption of a Privacy Program

Grantees that are not required to comply with HIPAA or analogous state patient privacy laws may still refer to such laws for highlights on best practices for voluntary privacy programs, including an emphasis on patient consent and control of their information, minimum necessary standards (i.e., limiting information disclosures to the minimum amount necessary to accomplish an intended purpose), and implementation of certain safeguards.

At a minimum, a privacy program should involve:

- Conducting a risk assessment that reviews the scope of individual information available to the grantee, permissible and required disclosures and uses of information within the Produce Prescription project, and privacy and security vulnerabilities. The risk assessment should be documented. The federal Office of the National Coordinator for Health Information Technology and the U.S. Department of Health and Human Services developed a security risk assessment tool that may be helpful. (Visit healthIT.gov for more information and to access the resource, *Security Risk Assessment Tool*).
- Developing and implementing a written policy that details how the grantee will respond to the risks identified in the assessment with a focus on strategies to minimize vulnerabilities.

> Grantees can ask themselves the following questions when considering how to integrate protections into their everyday operations:
> - What sort of information do we need to collect from participants to provide our services? What sort of information is unnecessary for us to collect?
> - How can we collect, share, or use personal health information in a way that respects an individual's autonomy and their right to control their own information?
> - How do we store information in a way that protects it from being seen by people who should not have access to it?

Patient Privacy and Technology Platforms

Grantees and grantee partners exploring privacy programming may hear about "HIPAA-compliant software" and "HIPAA compliance software." The term HIPAA-compliant software is used to refer to software that has incorporated the necessary HIPAA privacy and security safeguards into the way information is stored, retrieved, and transmitted (e.g., utilizing authentication mechanisms to verify users' identification, in order to support that someone accessing PHI is who they say they are, e-mail encryption to ensure the secure transmission of electronic PHI). HIPAA compliance software refers to software products that offer 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 grantees exploring this kind of product:

- There is no official certification program. When a company markets a product as HIPAA compliant, it is making a claim that the product includes all the necessary privacy and security safeguards to comply with HIPAA's requirement (typically based on the fact that the product was developed to meet HIPAA requirements specifically).
- HIPAA does not require that organizations invest in any particular technology solution(s). Not every organization has the capacity to use complex or expensive technology platforms to handle PHI, and grantee organizations must decide what security strategies will be most effective and feasible to adopt.
- Use of HIPAA-compliant software does not itself ensure HIPAA compliance. Organizations are still responsible for carrying out their compliance program, and for ensuring that the way they use any software comports with HIPAA.
- Many of the popular suppliers of organizational software packages/products, including Microsoft, Google, Slack, and Zoom, 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. Grantees 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. If the software vendor 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.

Case Study: Qualtrics and HIPAA Compliance
Qualtrics is an online survey tool that many grantees use for collecting and analyzing non-clinical, de-identified participant-level data. Even so, grantees may hear about how Qualtrics enables HIPAA compliance.

Qualtrics has HITRUST certification, meaning the company has certifiably demonstrated that products can be configured to include HIPAA-related controls. Qualtrics also can, and does, enter into Business Associate Agreements with organizations subject to HIPAA.

This does not, however, mean that the platform automatically ensures HIPAA-related controls are built into the user experience or that a Business Associate Agreement is automatically entered into with the company. Also, as noted, the adoption of HIPAA-compliant software does not itself ensure HIPAA compliance. Organizations are still responsible for carrying out their compliance program, and for ensuring that the way they use any software comports with HIPAA.

Community Resource Referral Platforms

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

Point-of-Sale Technology and HIPAA

Grantees often rely on point-of-sale technology platforms to facilitate transactions at participating retailers. In general, these platforms work with de-identified data/do not work with PHI. This means that special security measures relating to HIPAA are not required.

About

Acknowledgments

The Center for Health Law and Policy Innovation of Harvard Law School (CHLPI) advocates for health and food justice, with a focus on the needs of systemically marginalized individuals. CHLPI works with a range of stakeholders to expand access to high-quality health care and nutritious, affordable food; to reduce health and food-related disparities; and to promote more equitable and sustainable health care and food systems. 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.

GusNIP NTAE staff and University of California San Francisco consultants reviewed and edited the briefs for alignment with GusNIP goals and activities.

Suggested Citation

Landauer, R. and Downer, S. (2022, January). *HIPAA Issue Brief 5 - Developing a Privacy Program.* GusNIP NTAE Center, Nutrition Incentive Hub. https://www.nutritionincentivehub.org

nutritionincentivehub.org
info@nutritionincentivehub.org

The Nutrition Incentive Hub

The Nutrition Incentive Program Training, Technical Assistance, Evaluation, and Information (NTAE) Center is led by the Gretchen Swanson Center for Nutrition. In partnership with Fair Food Network, they created the Nutrition Incentive Hub, a coalition of partners to support this work. These partners are practitioners, retail experts, researchers, and evaluators from across the country bringing decades of experience and leadership in technical assistance, training, reporting, and evaluation. The Nutrition Incentive Hub is dedicated to building a community of practice to maximize program impact and ensure that all Americans have access to the healthy foods they need.

This work is supported by Gus Schumacher Nutrition Incentive Grant Program (GusNIP) Nutrition Incentive Program Training, Technical Assistance, Evaluation, and Information Center (NTAE) [Grant no. 2019-70030-30415/project accession no. 1020863 from the United States Department of Agriculture (USDA) National Institute of Food and Agriculture]. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the view of USDA.