



Data Sharing to Build Effective and Efficient Benefits Systems

A Playbook for State and Local Agencies

By Jeneé Y. Saffold, Bridget Gibbons Straughan, Alissa Weiss

Funded by the Walmart Foundation

JANUARY 2023

Forward from BDT's Chief Executive Officer

Nearly 20 years ago, Benefits Data Trust (BDT) began a journey to make it easier for eligible individuals and families to connect to critical resources. Joining forces with the Pennsylvania Department of Aging, we began using data sharing to conduct proactive outreach to older adults who were eligible for low-cost prescription medication. To date, this innovative partnership has allowed us to facilitate **more than 240,000 enrollments in the Pharmaceutical Assistance Contract for the Elderly (PACE) Program**, helping to improve the wellbeing of older adults throughout the Commonwealth of Pennsylvania. Since then, we have used this approach with other states and benefits, facilitating nearly 800,000 benefit enrollments for families and individuals nationwide.

There was no blueprint when we began this initiative — we wrote it. At that time, harnessing the power of data to help bolster enrollment in benefit programs was considered cutting-edge. Today, the landscape is much different; advanced data sharing pilots and long-sustained efforts are occurring in government agencies and institutions all across the country. By using data, we have the opportunity and ability to break through the programmatic silos and administrative barriers that lead eligible families to miss out on critical assistance each year. BDT is proud to be a leader in that widespread work today.

To implement effective data sharing, agencies don't need to have perfect data or the most up-to-date data infrastructure. Initiatives that make a tremendous impact can start with just a spreadsheet and a commitment to working across teams to build understanding and trust.

Now more than ever, the value of making government systems more efficient and equitable is clear. So is the need to streamline families' access to vital assistance. With an estimated **\$80 billion in critical assistance currently untapped**, it's crucial that we better connect under-enrolled populations and address prevalent barriers, like staffing issues within state agencies, in doing so. Data sharing can help us to reach new, and necessary, heights.

Through months of work and interviews with experts and administering agencies, our team has gathered invaluable information on data sharing and how it can help us address critical, yet solvable issues in benefits access. We're excited to share these insights with the field and hope to continue to engage our peers, share learnings, and build pathways to more equitable systems for all.

— Trooper Sanders, CEO



Credits and Thanks

This Playbook was written by Jeneé Y. Saffold, Policy Attorney; Bridget Gibbons Straughan, Government Innovation Manager; and Alissa Weiss, Director of Government Innovation at BDT. Thank you to BDT interviewees, reviewers, content contributors, and everyone else at BDT whose generous time and insights were invaluable to its development:

Pauline Abernathy, Edmund Aristone, Stephanie Baker, Lura Barber, LaKisha Bowman, Vanessa Burkhardt, Lucas Caldwell-McMillan, Conor Carroll, John Cianfrani, Alexis Clark, Tim DeSario, Lisa Dillman, Mary Falls-Staley, Kayla Gaskin, Marcia Gelbart, Rachel Gershon, Ashley Humienny, Jillian Humphries, Paul Huntsberger, Michael Johnson, Julia Kosov, Ryan Lauko, Elizabeth Lawler, Brett Lear, Miriam Lipschutz, Kaley Maltz, Jamila McLean, Marta Miguel, Lauren Phillips, Jamie Renman, Caiti Roth-Eisenberg, Alejandra Solorzano, Neeta Sonalkar, Wanja Thuku, Morgan Vierling, Julian Xie, Elisa Zygmunt.

Thank you to our external interviewees and reviewers for your valuable insights, comments, and suggestions:

Anna-Maria Galli, Alex Naismith, Kevin Tabor, University of Pittsburgh Medical Center (UPMC); Eric Gianella, Code for America; Amy Hawn Nelson and Deja Kemp, Actionable Intelligence for Social Policy, University of Pennsylvania (AISP); Hilary Heishman, Robert Wood Johnson Foundation (RWJF); Matthew Klein, Robin Hood Foundation; Khaliyl Lane, LinkedIn; Jess Maneely and Matt Lyons, American Public Human Services Administration (APHSA); Bill Marella, HealthShare Exchange (HSX); Tom Snedden, Pennsylvania Department of Aging, Pharmaceutical Assistance Contract for the Elderly (PACE); Matt Stevens, Hawai'i Workforce Funders Collaborative; Anh Tran, Washington State Department of Health, Office of Nutrition Services; Tayyab Walker, New York City Office of Technology and Information; Steph White, Michigan Department of Health & Human Services; Ginger Zielinskie, Evergreen Strategic Advisors.

Support for this Playbook was provided by a grant from the Walmart Foundation.

Thank you to Zoë Neuberger, Senior Policy Analyst at the Center on Budget and Policy Priorities, and Caiti Roth-Eisenberg, Policy Manager at BDT, for their work on the toolkit *Increasing WIC Coverage Through Cross-Program Data Matching and Targeted Outreach*,¹ which greatly informed and influenced the content of the Playbook. Thank you to One Degree for their foundational report, *Maximizing Linkages: A Policymaker's Guide to Data Sharing*,² which provided helpful insight for this piece. Thank you to the Center for Health Care Strategies (CHCS) for their collaboration on the forthcoming resource about inter-agency data sharing, whose insights informed parts of this Playbook; and thank you to the Robert Wood Johnson Foundation (RWJF) for their funding and support of that initiative.

The findings and conclusions contained within are those of the authors and do not necessarily reflect the positions of the funders, reviewers, interviewees, or entities whose examples are cited throughout the Playbook.

NOTICE: The information provided in this Playbook is not intended to constitute legal advice; instead, all information and content in this Playbook are for general informational purposes only. Although this information is accurate as of the date of this publication, it may not constitute the most up-to-date legal or other information at the time it is read. You should consult your legal counsel to obtain advice with respect to any legal matter. Do not act or refrain from acting based on information in this Playbook without first seeking legal advice from your legal counsel in the relevant jurisdiction.

¹ Center on Budget & Policy Priorities and Benefits Data Trust, "Toolkit: Increasing WIC Coverage Through Cross-Program Data Matching and Targeted Outreach," March 2022, [Weblink](#).

² Khaliyl Lane, "Maximizing Linkages: A Policymaker's Guide to Data-Sharing," One Degree (formerly Alluma), April 10, 2019, [Weblink](#).





Table of Contents

Forward from BDT’s Chief Executive Officer	2
Credits and Thanks	3
Table of Contents	4
Roadmap to Using this Playbook	5
Executive Summary	6
Glossary	8
Section 1: Introduction	10
Section 2: Making the Case: The Power of Data Sharing for Analysis and Outreach	14
Section 3: The Building Blocks of Data Sharing: Law, Privacy and Security, and Data Sharing Agreements ...	19
Key Legal, Privacy, and Security Concepts in Data Sharing	20
Legal Considerations	21
Understanding the Approach to Legal Analysis	21
Overarching Federal Privacy Laws	23
Federal Benefits Laws	24
Telephone Consumer Protection Act and Texting Outreach	27
Crafting the Data Sharing Agreement	30
Section 4: How to Plan, Launch, and Scale a Smooth and Efficient Data Sharing Process	32
Aligning on Purpose and Goal	35
Pulling Together the Team	36
Implementation Considerations that Inform the Data Needs	38
Selecting Data Fields	39
Conducting Evaluations	40
Working with the Data	41
Sustain and Scale	45
Section 5: Collaborating with Other Sectors	46
Healthcare.....	47
Higher Education	50
Community Outreach Partners	53
Research	54
Appendix	56
Appendix I: Data Sharing Agreement Shells	57
Appendix II: Sample Data Sharing Agreements	72
Appendix III: Additional Resources	101





Roadmap to Using This Playbook

Benefits Data Trust has designed this Playbook as a “how-to” guide for using data sharing to make benefit systems more effective and efficient. This resource is primarily written for program directors, project managers, policy staff, and others from the city, county, and state government agencies that administer benefits. The goal is to help individuals in those roles work with agency executives, legal and data teams, and other key stakeholders to scope and design successful data sharing projects. While largely focused on data sharing within and across administering agencies, the Playbook also includes information about data sharing with community outreach partners, as well as the healthcare, higher education, and research sectors. We hope this Playbook also provides value to staff from those institutions.

No matter where you are in your data sharing journey, we want this Playbook to be helpful to you and encourage you to explore the sections in whatever order is most valuable to you. Below are suggestions about how to use the Playbook based on the core questions you’re trying to answer:

Are you new to data sharing and want to understand the basics? Are you trying to figure out if data sharing can help achieve your goals for the benefits system? Check out:

 **Section 1** →

 **Section 2** →

 **Section 3** →

Are you looking to understand the legal, privacy, and security considerations of a data sharing project and want information that can inform conversations with your legal teams? Check out:

 **Section 3** →

Have you completed many data sharing projects and want to refine your approach and learn advanced tips and ideas? Check out:

 **Section 4** →

Are you just starting a data sharing project and want to walk through the key steps and best practices to launch a project? Check out:

 **Section 3** →

 **Section 4** →

Are you a healthcare or higher education institution, community outreach partner, or researcher looking for a data sharing overview? Are you a government agency considering a partnership with another sector around benefits outreach? Check out:

 **Section 5** →

Are you interested in seeing data sharing agreement examples and shells you can use to inspire your own efforts? Are you looking for more resources on data sharing? Check out:

 **Appendix** →

Remember, BDT is available to you as a resource. To discuss any topics in more detail or ask questions, please reach out to us at partnerships@bdtrust.org.





Executive Summary

Research has consistently documented many positive impacts of participating in social safety net programs like the Supplemental Nutrition Assistance Program (SNAP) and Medicaid, from improved health outcomes^{1,2} to strengthening local economies.³ Despite these positive outcomes, many programs are chronically under-enrolled. More than \$80 billion in benefits to pay for food, healthcare, broadband, and more go untapped each year. **When conducted with appropriate and responsible safeguards, data sharing can help address these gaps in participation and build efficient, equitable benefits systems.**

Data sharing for analysis and outreach can illuminate who is not accessing benefits, better connect under-enrolled populations to vital assistance, and make the system more efficient for administering agencies and participants alike. *Data Sharing to Build Effective and Efficient Benefits Systems: A Playbook for State and Local Agencies* is focused on how government and other key sectors can use data sharing to identify individuals who are eligible but unenrolled in benefits, understand gaps and disparities in access, and use outreach to help eligible individuals connect to and maintain their benefits.

Agencies do not need to have perfect data or the most modern data infrastructure to develop secure data sharing initiatives that benefit residents and frontline workers. This kind of data sharing is happening all over the country — innovative pilots and long-sustained efforts exist in agencies and institutions across red, purple, and blue states. Yet these proven approaches are underutilized due to legal, privacy, or security concerns about data sharing as well as operational hurdles related to using administrative data from siloed programs and aging infrastructure.

This Playbook is designed to help the government and others address these issues in order to run secure and effective data sharing initiatives. It provides legal analysis regarding the laws governing data sharing as well as step-by-step guidance to make the process sustainable and scalable. The Playbook contains additional data sharing resources, including case studies and data sharing agreement (DSA) examples. It was informed by BDT's nearly 20 years of experience with data sharing, as well as interviews with 35 federal, state, and local officials and other experts from the fields of benefits access and data sharing.

The entryway to any data sharing project is the fundamental question: does the law permit data sharing for this specific circumstance? This Playbook provides key context on how to answer this question and navigate the legal process surrounding data sharing.

- » A successful data sharing endeavor can improve the benefits system while following the legal, privacy, and security rules that are necessary for the lawful and ethical use of confidential data. Most benefit program laws specify whom applicant/participant data may be shared with and for what purposes. Understanding those laws and considerations can unlock the potential of data sharing.



- » A combination of state and federal privacy laws, benefits laws, and outreach medium laws must be consulted to assess whether data sharing is permitted for a specific use case. This Playbook includes relevant federal privacy laws, federal benefits laws, and federal law pertaining to SMS text-based outreach. The analysis focuses on SNAP, Medicaid, WIC, Low Income Home Energy Assistance Program (LIHEAP), and Unemployment Compensation (UC) because many of these programs have overlapping eligibility requirements and have shown great promise for data sharing activities.
- » A strong data sharing agreement (DSA) – the legal document that governs data sharing practices – justifies the reason for sharing the data, explains what is being done with the data, and describes the approaches to safeguarding and protecting the data. It serves as the common understanding between the relevant parties and can be written in a way that allows for ongoing operational adjustments.

While data sharing projects start with a focus on legal authorities, data security, and privacy, there are steps agencies can take to implement a smooth and efficient data sharing process. Key recommendations include:

- » Engage executive sponsors and key stakeholders – especially legal, programmatic, and data teams – early in the process. Impactful initiatives can start with just an Excel spreadsheet, as long as there is a commitment to building understanding and trust across teams.
- » Plan which fields are needed to conduct analysis, outreach, and evaluation to ensure that the DSA includes the data needed to run the intervention and measure success. Defining a clear purpose for each data field will also help expedite the legal review.
- » Include demographic and geographic data in the DSA in order to understand disparities in access, build person-centered interventions, assess whether interventions are working for different populations, and adjust outreach to build a more equitable system.
- » Develop a shared understanding around the definitions and formats of the data being shared; this is a worthwhile investment that makes the sharing, matching, and analysis process significantly easier.
- » Involve non-governmental sectors and partners in data sharing efforts to build a stronger benefits system. Healthcare entities, higher education institutions, and community outreach partners are particularly well-positioned to reach individuals who are likely eligible for benefits. Research partners can build evidence regarding connections between benefits participation and health, education, and economic outcomes.

Through guidance like this and more, BDT hopes this publication can support and inspire data sharing initiatives across the country. For questions and assistance, we encourage government agencies and other institutions interested in data sharing for analysis and outreach to contact us at partnerships@bdtrust.org. We are eager to support readers' efforts to build more efficient and equitable benefits systems.





Glossary

When teams involved in data sharing projects align on a shared vocabulary, it helps them to execute effectively. As such, we offer definitions for key terms that will appear throughout the Playbook. Attribution is included where relevant, although some definitions have been modified for the context of this discussion.

Administering agencies: government departments that administer one or more government-funded program(s). As it relates to public benefits, their responsibilities include determining the eligibility of households and individuals for benefits, enrolling eligible individuals in benefits, providing household benefits, and ensuring program integrity (*adapted from [U.S. Department of Agriculture, Food and Nutrition Service](#)*).

Administrative data: information about individuals or households that is collected and maintained as part of the operation of government programs (*adapted from [Actionable Intelligence for Social Policy, University of Pennsylvania](#)*).

Community outreach partner: entities that are external to government such as social service providers or community-based organizations (CBOs) that help eligible members of their constituencies connect to benefits through activities like outreach and assistance with benefits applications.

Data dictionary: a collection of names, definitions, and attributes about data elements that are being used or captured in a database or information system. It describes the meanings and purposes of data elements within the context of a project, and provides guidance on interpretation about data elements (*adapted from [UC Merced Library](#)*).

Data governance: the people, policies, and procedures that support how data are managed, used, and protected. The purpose of data governance is to help organizations formally manage and gain better control over their data to balance security with accessibility (*adapted from [Actionable Intelligence for Social Policy, University of Pennsylvania](#) and [Dataversity](#)*).

Data matching: the process of comparing data across data sets and finding records that refer to the same person, entity, or case (*adapted from [Integrate.io](#)*).

Data privacy: the ability of individuals to control the storage, access, sharing, retention, and immutability of their personal information.

Data security: the protection of information to prevent loss and unauthorized access. It consists of the processes that assess threats and risks to information, as well as the procedures and controls needed to preserve the confidentiality, integrity, and availability of information.

Data sharing: the process of providing other agencies or entities with access to information that they cannot already access in their own systems. For the purposes of this Playbook, the focus is individual-level data about benefits participation (*adapted from [Actionable Intelligence for Social Policy, University of Pennsylvania](#)*).



Data sharing agreement (DSA; also called “data use agreement”): a contractual agreement between two or more partners that sets out the legal authority to support data sharing, establishes and documents the terms and conditions, and delineates monitoring and responsibility (*adapted from [The Network for Public Health Law](#)*).

Data transfer: the process by which data is sent and received. The parameters for this process are typically described in a data sharing agreement, including how the process will comply with all legal obligations to secure and protect the data.

Outreach: communications sent to individuals to convey information or request they take an action. For the purposes of this Playbook, the focus of the outreach is around letting individuals know they are likely eligible for benefits and how to apply, or to share information about their current benefit status and how to maintain benefits. Outreach can be sent via several modalities including text messages, phone calls, or mail.

Unique identifier: a sequential number, label, or code that is assigned to each record in a data file to distinguish their information from other records. For example, a Social Security Number or other randomly assigned number is used to differentiate one person’s information from others who may share some identifying information but are distinct people or cases.

Use case: a unique instance of sharing a specific type of information. Each use case describes the purpose, type of data exchanged, and rules for interactions between people and systems. It also outlines the technical and legal frameworks required to share the information (*adapted from [Michigan Health Information Network](#)*).

Throughout the Playbook, we will reference various benefit programs, some of which are known by their acronym:

- Affordable Connectivity Program (ACP)
- Low Income Heating Assistance Program (LIHEAP)
- Medical Assistance (MA) or Medicaid
- Supplemental Nutrition Assistance Program (SNAP)
- Supplemental Nutrition Assistance Program for Women, Infants, and Children (WIC)
- Unemployment Compensation (UC)





SECTION 1




Introduction

Social safety net programs like the Supplemental Nutrition Assistance Program (SNAP), the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC), and Medicaid are powerful tools that provide children, older adults, and families access to food, medicine, and other vital resources. These programs are a bulwark in economic downturns: they reduce material hardship,³ have stabilized individuals and families during the COVID-19 pandemic, and remain crucial in the face of global inflation and economic instability.

³ Signe-Mary McKernan, Caroline Ratcliffe, Breno Braga, "The effect of the US safety net on material hardship over two decades," *Journal of Public Economics* (Vol. 197), May 2021, [Weblink](#).

Moreover, research has consistently documented many positive impacts of participating in benefit programs, from reductions in hospitalization and nursing home admissions,⁴ to saving \$2,360 per patient in Medicaid spending,⁵ to improved child welfare⁶ and educational outcomes.^{7,8} Benefits strengthen local economies as well: every \$1.00 in SNAP benefits has been found to generate an estimated \$1.50 to \$2.00 in economic activity.⁹

Despite these positive outcomes, many programs are chronically under-enrolled. More than **\$80 billion in benefits** to pay for food, healthcare, broadband, and more go untapped each year.¹⁰

-  **1.3 million seniors** are eligible for but not enrolled in Medicare Extra Help prescription drug assistance (also known as the Part D Low income Subsidy, or LIS)¹¹
-  **43%** of eligible parents and young children are not enrolled in WIC¹²
-  **More than a quarter of the eligible working poor (26%)** are not enrolled in SNAP¹³

Data sharing can help address these gaps in participation.

For nearly 20 years, Benefits Data Trust (BDT) has harnessed the power of data, policy, and technology to provide efficient and dignified access to assistance. A cornerstone of BDT's work is identifying individuals who are enrolled in one means-tested program but are eligible for more, and helping them access additional assistance. For example, we have helped agencies use data to identify Medicaid recipients who are not receiving SNAP – even though the eligibility criteria are similar – and send outreach to connect those individuals to food assistance. We have executed 40 data sharing agreements (DSAs) with cities, states, healthcare entities, and institutions of higher education in service of this work, which has allowed us to facilitate approximately 800,000 benefit enrollments and secure over \$9 billion in assistance for families and individuals nationwide.

-
- ⁴ Laura J Samuel, Sarah L Szanton, Rachel Cahill, Jennifer L Wolff, Pinchuan Ong, Ginger Zielinskie, Charles Betley, "Does the Supplemental Nutrition Assistance program affect hospital utilization among older adults? The case of Maryland," *Population Health Management* (Vol. 21, No. 2), April 2018, [Weblink](#).
 - ⁵ Seth A. Berkowitz, Deepak Palakshappa, Joseph Rigdon, Hilary Seligman, Sanjay Basu, "Supplemental Nutrition Assistance Program Participation and Health Care Use in Older Adults," *Annals of Internal Medicine*, December 2021, [Weblink](#).
 - ⁶ Michelle Johnson-Motoyama, Donna K. Ginther, Patricia Oslund, "Association Between State Supplemental Nutrition Assistance Program Policies, Child Protective Services Involvement, and Foster Care in the US, 2004-2016," *Jama Network Open*, July 13, 2022, [Weblink](#).
 - ⁷ Hilary Hoynes, Diana Whitmore Schanzebach, Douglas Almond, "Long-Run Impacts of Childhood Access to the Safety Net," *American Economic Review* (Vol. 106, No.4), April 2016, [Weblink](#).
 - ⁸ Heather Novack, Lyle McKinney, "The Consequences of Leaving Money on the Table: Examining Persistence among Students Who Do Not File a FAFSA," *Journal of Student Financial Aid* (Vol. 41, Issue 3, Article 1), 2011, [Weblink](#).
 - ⁹ Patrick Canning, Brian Stacy, "The Supplemental Nutrition Assistance Program (SNAP) and the Economy: New Estimates of the SNAP Multiplier," U.S. Department of Agriculture, Economic Research Services, July 2019, [Weblink](#).
 - ¹⁰ BDT estimate based on federal data and reputable third-party sources.
 - ¹¹ Social Security Administration, "Social Security Administration (SSA) Annual Data for Outreach to Low-Income Medicare Beneficiaries Extra Help and Medicare Savings Programs L447 & L448 Notices," May 11, 2022, [Weblink](#).
 - ¹² U.S. Department of Agriculture, Food and Nutrition Services, "WIC 2019 Eligibility and Coverage Rates," April 4, 2022, [Weblink](#).
 - ¹³ U.S. Department of Agriculture, Food and Nutrition Services, "Reaching Those in Need: Estimates of State Supplemental Nutrition Assistance Program Participation Rates in 2018," May 19, 2021, [Weblink](#).



Data sharing is at the heart of this proven approach. **When conducted with appropriate and responsible safeguards, data sharing is a powerful tool** that government agencies and other key sectors can deploy to ensure that eligible people receive assistance efficiently and equitably. Government agencies can use data in a variety of ways to strengthen and streamline their benefit systems. Existing participant data can be used to facilitate enrollment in other programs, auto-populate application and renewal forms, or reduce verification requests by relying on information already on-hand.

This Playbook is specifically focused on data sharing for analysis and outreach. By this we mean:

- » Sharing individual-level data across benefit programs with similar eligibility criteria and conducting a data match to identify individuals who are on one benefit but not another, and therefore likely eligible for other benefits
- » Analyzing the results of that data match to better understand the size of the enrollment gaps as well as any demographic and/or geographic enrollment trends
- » Sending outreach to likely eligible individuals to raise awareness of benefits and share steps about how to apply; and/or help current recipients take critical steps to maintain their benefits

Efforts like this have helped illuminate who is not accessing benefits, better connect under-enrolled populations to vital assistance, and make the system more efficient for administering agencies and participants alike.

This kind of data sharing exists all over the country — innovative pilots and long-sustained efforts are occurring in agencies and institutions of all sizes in red, purple, and blue states. For example:

- » BDT and the Center for Health Care Strategies conducted a forthcoming national survey of SNAP and Medicaid administrators. Of 46 responding states, at least **18 indicated they currently share data across Medicaid and SNAP to conduct outreach.**
- » The Center on Budget and Policy Priorities' 2022 survey of WIC agencies found that **29 state agencies were using Medicaid and/or SNAP data to identify WIC enrollment gaps and 13 states** were using Medicaid or SNAP data for outreach, with six more preparing to launch outreach.¹⁴

¹⁴ Zoë Neuberger, Lauren Hall, "WIC Coordination With Medicaid and SNAP," Center on Budget and Policy Priorities, November 14, 2022, [Weblink](#).



Agencies do not need perfect data or the most modern data infrastructure to begin experimenting with data sharing; initiatives that make a tremendous impact can start with just an Excel spreadsheet and a commitment to working across teams to build understanding and trust.

While these approaches help administering agencies provide efficient and comprehensive services to participants and individuals in need, they are underutilized. Some agencies question whether they have the legal authority necessary for data sharing or have privacy and security concerns about sharing individual-level data. Concerns about protecting individuals' privacy and data are both valid and necessary. Every data sharing effort must be supported by rigorous data security measures that protect the personal information of applicants and participants. BDT has seen that it is possible for agencies to balance the twin goals of protecting people's personal data and connecting them to the benefits and services they may need.

BDT's Playbook provides a roadmap for government agencies and other sectors to find that balance. This step-by-step guide is informed by BDT's own experience as well as interviews with 35 city, state, and federal officials and other experts in the benefits access and data sharing space. It arms readers with the issues they need to consider and discuss with agency lawyers, administrators, and other relevant stakeholders to ensure that data sharing is permissible and secure, and includes tools to guide and inspire efforts in your institution. We hope this resource benefits your teams as well as the residents and communities you serve.





SECTION 2

Making the Case: The Power of Data Sharing for Analysis and Outreach

Why engage in data sharing for analysis and outreach?

Data sharing can help agencies...

- **Understand the scale of participation gaps** between benefit programs to determine the value and/or need for cross-enrollment efforts
- **Uncover disparities in benefits access** to see if there are populations with disproportionately low rates of enrollment
- **Increase benefit participation through outreach** to all likely eligible individuals or specific priority populations (e.g., seniors, college students, etc.)
- **Deliver efficient services** that streamline the process for agencies and residents alike
- **Work with a community outreach partner** that has strong ties to particular communities and can quickly and flexibly deploy outreach efforts

At a time when human services agencies are being called upon to build more efficient systems that reduce burdens on both frontline workers and participants, we must find solutions that help us do so. Data sharing can be one of those vital solutions. Data sharing also connects individuals to a holistic set of supports, which is particularly important to healthcare and social service institutions focused on the critical role of the social drivers of health (SDOH).

“ Families don't try to engage piecemeal with different parts of government. They exist as holistic entities who experience the public sector, and the public sector should be as coordinated as possible to make that experience as helpful as possible. All of those things require backend coordination across agencies, and backend coordination means data sharing. ” - **Former Government Operations Administrator**

By sharing data and comparing lists of benefit recipients, it is possible to **identify hundreds of thousands of individuals** who are missing out on more comprehensive assistance. Simply conducting a data match across programs can help agencies and institutions looking to understand cross-enrollment participation gaps. BDT and CBPP worked with four states using data sharing and matching across programs to increase WIC enrollment. Conducting statewide data matches to identify individuals participating in Medicaid and/or SNAP but not WIC revealed astonishing cross-enrollment gaps ranging from 44 percent to 77 percent.¹⁵

Armed with that kind of information, many administering agencies choose to deploy outreach to address the gaps they find, and this outreach has proven to be incredibly effective. For example:

- » A peer-reviewed study found that conducting **SNAP outreach to Medicaid enrollees aged 60 and older led to an 83% increase in SNAP participation.**¹⁶
- » Low-cost text outreach to individuals on Medicaid has been found to increase enrollment in WIC, helping states address declining WIC participation rates amongst eligible families.¹⁷
- » Sending outreach to current SNAP and Medicaid participants about the steps they need to take to recertify and maintain their benefits is a powerful way to reduce “churn” — when otherwise eligible households become unenrolled due to administrative hurdles, creating the need for them to reapply shortly thereafter.^{18, 19}

¹⁵ Jess Maneely, Zoë Neuberger, “Matching Data Across Benefit Programs Can Increase WIC Enrollment,” Center on Budget and Policy Priorities and Benefits Data Trust, April 27, 2021, [Weblink](#).

¹⁶ Amy Finkelstein, Matthew Notowidigdo, “Take-Up and Targeting: Experimental Evidence from SNAP,” The Quarterly Journal of Economics (Vol. 134, Issue 3), August 2019, [Weblink](#).

¹⁷ Jess Maneely, Zoë Neuberger, “Using Data Matching and Targeted Outreach to Enroll Families with Young Children in WIC: Lessons Learned from State Pilots,” Center for Budget and Policy Priorities and Benefits Data Trust, January 5, 2021, [Weblink](#).

¹⁸ Katie Sullivan, Sara Soka, Keith Barnes, “Text to Connect: Using Text Message Outreach to Reduce SNAP Churn,” Benefits Data Trust and Beeck Center for Social Impact + Innovation at Georgetown University, October 2021, [Weblink](#).

¹⁹ Kindra Serafi, Alex Dworkowiz, Michael Budros, “Text Messaging: An Important Communication and Outreach Strategy as States Unwind the Federal Medicaid Continuous Coverage Requirement,” State Health & Value Strategies, January 28, 2022, [Weblink](#).



Data sharing provides a powerful opportunity to **better understand disparities in the benefits system** and can help build equitable solutions to address those gaps. By using data to answer questions like “which populations are underserved?” and “who is and who is not responding to this outreach?” it is possible to deliver better, more equitable services. Agencies can design outreach strategies that prioritize specific populations, including seniors, students, veterans, families with young children, rural residents, non-English speakers, and more. This approach also allows government to serve participants holistically, acknowledging that the individual who is food insecure likely needs affordable medical care and utility assistance as well.

Agencies also benefit from the efficiencies of data sharing and outreach. Individuals who have already been deemed eligible for other means-tested benefits likely qualify for additional programs, making this kind of outreach economical and effective. Outreach campaigns can also be used to smooth out and manage workloads. For example:

- » Outreach can be staggered to control the inbound flow of applications. One agency that worked with BDT to send SNAP recertification reminders found that the campaign prevented spikes in participant responses, making it easier to manage workload while reducing the likelihood of churn.
- » Outreach to families who are automatically income-eligible for WIC because they participate in Medicaid or SNAP simplifies the eligibility determination process and can reduce the number of documents that WIC staff need to review.²⁰

Sharing data and information across agencies can also position agencies to **navigate the introduction of federal waivers and major policy shifts**. From dramatically simplifying Medicaid enrollment during the Patient Protection and Affordable Care Act (ACA)-initiated Medicaid expansion²¹ to driving awareness about the new broadband benefit, the Affordable Connectivity Program (ACP),²² data sharing is a critical tool for agencies. This is the case as states prepare for the end of the COVID-19 Public Health Emergency (PHE). Data sharing is facilitating efforts across agencies, Medicaid managed care organizations (MCOs), and community partners to update enrollee contact information and send outreach to help people retain access to healthcare.²³

“ There’s this idea of ‘we’ve got to get our house in order before we can start to talk about data sharing.’ But if you structure it right, you can actually use data sharing to help everyone get their house in order at the same time. Wherever you are right now is good enough. ” - Data Sharing Practitioner

²⁰ Jess Maneely, Zoë Neuberger, “Using Data Matching and Targeted Outreach to Enroll Families with Young Children in WIC: Lessons Learned from State Pilots,” Center for Budget and Policy Priorities and Benefits Data Trust, January 5, 2021, [Weblink](#).

²¹ Jessica Maneely, Caiti Roth-Eisenberg, “Issue brief- Fast Track: A quicker road to Medicaid enrollment,” Benefits Data Trust, February 5, 2020, [Weblink](#).

²² The White House, “Vice President Harris Marks Important New Milestone in Administration’s Efforts to Cut Costs for American Families [Fact Sheet],” July 21, 2022, [Weblink](#).

²³ Pauline Abernathy, “Helping States and Families Prepare for the End of the Pandemic Emergency Declaration,” Benefits Data Trust, April 7, 2022, [Weblink](#).



CASE STUDY:

Text-based Outreach in NYC

To reduce churn, **Benefits Data Trust (BDT)** partnered with the **New York City Department of Social Services** and **Robin Hood** to engage in a low-cost strategy to help SNAP recipients in New York City successfully complete the annual recertification process required to stay on the benefit.

The strategy sends targeted text messages to “nudge” recipients at the right time, with the right information, to help them through the recertification process. BDT also received funding from a USDA SNAP Process and Technology Improvement Grant to support this pilot. Since it was launched in 2017, this strategy has helped thousands of New Yorkers successfully recertify, and it has done it at one-third the normal cost of helping them re-apply after losing SNAP.²⁴ The NYC pilot served as the foundation of similar efforts that BDT is launching with additional states.

Despite these many benefits, some public servants are uncertain about conducting data sharing for analysis and outreach. Throughout our interviews, legal, privacy, and security issues were consistently identified as the biggest impediment to launching data sharing projects. Every data sharing effort requires a sophisticated understanding of federal, state, and benefit-specific laws as well as clear privacy and security protocols. **With careful planning, it is possible to manage risks associated with transferring or sharing data.**

Even after legal, privacy, and security considerations are addressed, the operational realities of data sharing can present challenges. Benefits are often housed in separate agencies and departments with different leaders, goals, and approaches to data sharing. Since cross-enrollment efforts are not required at the federal or state level and are rarely anyone’s sole responsibility, it can be hard to prioritize in resource-constrained environments. It can also be difficult to navigate program-specific data systems and technical processes, not to mention the different ways of defining and formatting data.

Yet our interviews consistently revealed that these challenges pale in comparison to the substantial and meaningful advantages that data sharing can bring to both individuals and agencies. **The rest of this Playbook provides step-by-step guidance to help agencies and institutions address these hurdles and launch safe and effective data sharing projects.**

²⁴ Ryan Lauko, “Nudging benefits access in the right direction,” Benefits Data Trust, May 9, 2018, [Weblink](#).



CASE STUDY:

Helping Seniors in Pennsylvania

Tom Snedden, Director of the PACE Program at the Pennsylvania Department of Aging,²⁵ has long championed data-driven strategies to help older Pennsylvanians receive the benefits for which they're eligible. When the prescription assistance program launched in 1983, Tom was charged with ambitious goals of quickly enrolling eligible households. Tom and his team pursued lists of Property Tax and Rent Rebate Program (PTRR) recipients — since the requirements for that program and PACE were so similar — and used outreach to those individuals to enroll 600,000 people in PACE within three months. This initial use of data sharing to support PACE enrollment was incredibly effective and suggested there were even more eligible Pennsylvanians who were not yet connected to PACE.

600,000

**enrolled within 3 months by
Pennsylvania in its prescription
drug assistance program using
data sharing in**

JUST 3 MONTHS

Fast forward to 2000: Warren Kantor, BDT's founder, had a chance to meet Tom. Warren previously worked in the financial services sector where he witnessed the power of data-driven marketing to consumers and wanted to use that strategy to reach individuals eligible for public benefits. Having helped his mother apply for benefits, he saw how challenging the process could be. Warren believed there was a chance to increase PACE enrollment via the proactive outreach Tom had piloted, and in 2005, BDT and Tom launched the PACE Application Center,²⁶ which helps seniors apply for the program over the phone.

BDT's collaboration with PACE over the past 17 years has been a source of innovation in data sharing, proactive outreach, and dignified service responsible for facilitating over 240,000 enrollments in PACE. It has made a substantial impact on the overall health and well-being of Pennsylvanians, as PACE enrollees have been shown to be admitted to nursing homes an average of two years later than those who did not receive prescription assistance.²⁷

Over time, the partnership has leveraged 16 lists from other programs and agencies, including the Departments of Revenue, Military and Veterans Affairs, and Agriculture. It has also helped Pennsylvania seniors connect to other public benefit programs like PTRR, SNAP, LIHEAP, the Medicare Savings Plan (MSP), the Senior Food Box Program, and more — all in one interaction. Not only has Tom's vision for data sharing unlocked important services for hundreds of thousands of Pennsylvania residents, but the strategies informed the model BDT has deployed with other benefit programs, populations, and states across the country.

²⁵ Pennsylvania Department of Aging, "PACE Program – Prescription Assistance," Accessed November 29, 2022, [Weblink](#).

²⁶ Benefits Data Trust, "PACE Application Center," Accessed November 29, 2022, [Weblink](#).

²⁷ Thomas Snedden et al., "Improved Health Status and Avoidance of Nursing Home and Waiver Entry among the Enrollment in the Pharmaceutical Assistance Contract for the Elderly Program (PACE)," unpublished application to Centers for Medicare and Medicaid, August 2011.





SECTION 3

The Building Blocks of Data Sharing: Law, Privacy and Security, and Data Sharing Agreements

A successful data sharing endeavor can improve the benefits system while following the legal and privacy rules that are necessary for ethical use of data. **This section provides the background on legal, privacy, and security issues so that programmatic staff can have productive and informed conversations with their legal, privacy, and security teams.** It also includes an overview of the relevant legal authorities that permit data sharing for analysis and outreach, as well as guidance on the key elements of a data sharing agreement.

Key Legal, Privacy, and Security Concepts in Data Sharing

“ We’re just trying to make sure we’re complying with all the [benefit] rules, not sharing more information than we need to while at the same time providing the easiest customer service as possible. I think that is the ultimate question for a human services agency. ”

- Government Human Services Administrator

Below is an overview of foundational data sharing concepts.

The Law and Confidentiality:

The entryway to a data sharing project is the fundamental question: does the law permit data sharing for this specific circumstance?

- » Most benefit program laws specify whom applicant/participant data may be shared with and for what purposes. Understanding how to navigate those considerations and laws can unlock the potential of data sharing.
- » Under the law there will be many considerations to determine if data sharing is allowed, including confidentiality under federal privacy laws, benefit-specific laws, medium-specific laws (i.e., via text, letter, etc.), and consent.

Data Privacy:

Data privacy is the ability of individuals to control the storage, access, sharing, retention, and immutability of their personal information.

- » The key domains are focused on roles and responsibilities for data owners, data stewards, and data custodians; laws, regulations, and rules; and inter-organization and agency agreements like Business Associate Agreements, data sharing agreements, etc.

Consent:

Consent generally refers to an individuals’ indication of assent to having their data shared or used for a specific purpose.

- » Benefit programs and general privacy laws typically include specific provisions outlining the purposes for which data can be shared with and without individual consent. The exact definition of consent changes depending on the specific laws being referenced.
- » **This Playbook focuses on situations where federal law permits data to be shared without individual consent.** It should be noted that more robust data sharing options — across programs and/or for different purposes — may be possible if consent is collected by the administering agencies.

Data Security:

Data security is the protection of information to prevent loss and unauthorized access.

- » It is a multi-dimensional process that includes legal, procedural, and physical components.

Legal Considerations: How the Law Applies to Data Sharing Projects

While legal issues are often cited as a barrier to sharing individual-level participant data for the purpose of analysis and outreach, they are not insurmountable. BDT has worked with many administering agencies to address legal concerns so they can launch successful data sharing projects.

The desire to use data sharing to improve program effectiveness and advance equity must be balanced with existing legal and privacy protections that ensure data are not improperly used. Agency staff designing a data sharing project will need to engage their legal teams early in the process to chart a path forward.

To support productive and collaborative conversations across teams, it can be helpful for everyone to have a shared understanding of the basic legal framework that governs this area of law, and the key legal questions at the heart of the project. It is not our intention to make readers experts in all aspects of data sharing law. Instead, **this section is designed to provide foundational information on the law as it relates to sharing individual-level participant data and serve as a springboard for conversations with legal teams as they grapple with these important questions.** The full legal analysis and ultimate determination will be up to agencies' legal teams.

UNDERSTANDING THE APPROACH TO LEGAL ANALYSIS

Legal teams will need to understand the purpose and structure of the data sharing project, as the permissions for sharing data vary depending on the intended purpose and structure of the project. They will focus on the following elements:

Key Legal Questions	Example: Medicaid/WIC outreach project
Who is sharing the data?	The Medicaid agency will share data with the WIC agency
Who is using the data?	The WIC agency will use the Medicaid participant data to filter out those who are already participating in WIC
What is the type of data being shared?	The type of data is Medicaid participant data
What is the purpose for which the data are being shared?	The purpose is conducting outreach to individuals participating in Medicaid and eligible for but not participating in WIC

It is important to note that changes in any of these variables could affect the outcome of the legal analysis.

Additionally, the agency lawyers will have an interest in the security of the data storage and transfers to make sure those processes comply with the law. **The legal and security teams will need to know how the data will be sent and stored securely.** There are several methods available for securely transferring files and encrypting or de-identifying datasets while enabling analysis and outreach. A Secure File Transfer Protocol (SFTP) is a commonly used approach that most administering agencies have the capacity to implement.

Legal teams will consider several applicable laws when considering a prospective data sharing project to determine whether the law permits data sharing for that specific case. This Playbook covers several types of laws, including:

- overarching federal privacy laws that impact data sharing activities
- federal benefits laws
- federal law pertaining to SMS text-based outreach

Our benefit-specific analysis focuses on SNAP, Medicaid, WIC, LIHEAP, and UC because many of these programs have overlapping eligibility requirements and have shown great promise for data sharing activities. Readers should note that states may have their own privacy, benefit, or medium-specific laws that apply.

This section represents just some of the possibilities of data sharing for analysis and outreach. It is important to remember that **even if legal barriers emerge, it doesn't always mean the data sharing project can't move forward. It just may not happen in the way you originally envisioned.** Any change in "the who" or "the purpose" of the project may lead to a different result regarding the permissibility of data sharing, unlocking ongoing opportunities to accomplish your benefits access goals (see "Promising Practices from the Field" on page 43).

Summary of Federal Benefits Laws:

	When is data sharing allowed?	Relevant laws
SNAP	Data can be shared with persons directly connected with the administration of SNAP, federal assistance programs, or federally-assisted state programs and for the purpose of such administration.	7 USCS § 2020(e)(8); and 7 C.F.R. § 272.1(c)(2)
Medicaid	Data can be shared with persons directly connected with the administration of the Medicaid plan.	42 U.S.C. § 1396a(a)(7); 42 C.F.R. Part 431; and 45 C.F.R. Parts 160 and 164
WIC	Data can be shared with persons directly connected with the administration of the WIC program who have a need to know the information for WIC program purposes.	7 C.F.R. § 246.26(d)
LIHEAP	States have broad flexibilities to share data since there are no federal restrictions. There may be applicable state restrictions.	42 U.S.C.S. §§ 8621-8630 (2021) and regulations in 45 C.F.R. Part 96 Subparts A-F and H and 45 C.F.R. Part 75
UC	Data can be shared with public officials for use in their official duties.	20 C.F.R. Part 603



OVERARCHING FEDERAL PRIVACY LAWS

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is a federal law that required the creation of federal regulations to protect the privacy and security of certain health information. To this end, the U.S. Department of Health and Human Services created two sets of regulations: the Standards for Privacy of Individually Identifiable Health Information (the HIPAA Privacy Rule) and Security Standards for the Protection of Electronic Protected Health Information (the HIPAA Security Rule). The HIPAA Privacy Rule created national standards to protect individuals' medical records and other individually identifiable health information.²⁸ The HIPAA Security Rule created national security standards for protecting certain health information that is held or transferred in electronic form.²⁹ Individually identifiable information, referred to as Protected Health Information (PHI), is protected under HIPAA with rules and restrictions for disclosure.³⁰

What it means for data sharing for analysis and outreach:

If benefit program data is PHI, you must analyze whether the disclosure is permitted under HIPAA. Medicaid data needed for benefits analysis and outreach is commonly PHI. Reasons Medicaid PHI may be disclosed under HIPAA are discussed below (see "Medicaid Laws" on page 25-26).

The Privacy Act of 1974

The Privacy Act of 1974 is the federal law governing the handling of personal information in the federal government, including what records are collected, maintained, used, or disseminated by a federal agency.³¹

What it means for data sharing for analysis and outreach:

Because the Privacy Act applies to federal agencies sharing data, this Act does not impact data sharing activities at the state and local level, which is the focus of this Playbook.³²

Confidentiality of Substance Use Disorder Patient Records (42 C.F.R. Part 2)

Part 2 is the federal law protecting the privacy rights of people who seek treatment for substance use disorders from federally assisted programs.^{33,34} Part 2 places restrictions on federally-assisted programs regarding the disclosure of records that "would identify a patient as having or having had a substance use disorder" and "[c]ontain drug abuse or alcohol abuse information obtained by a federally assisted drug abuse program."³⁵

What it means for data sharing for analysis and outreach:

Part 2 does not generally apply to state or local agency data sharing projects, but agency legal teams may refer to the regulation when considering how to approach the sharing of information around addiction (e.g., sharing data about enrollment in a program whose eligibility criteria includes substance use disorder).

State Privacy Laws

Some states have specific privacy laws that will apply to data sharing projects. Where appropriate, your legal team will also consult these laws to determine if your specific data sharing projects are permissible.

²⁸ 45 CFR Part 160 and Subparts A and E of Part 164 (2021).

²⁹ 45 CFR Part 160 and Subparts A and C of Part 164 (2021).

³⁰ 45 C.F.R. 164.502 (2021).

³¹ 5 U.S.C.S. § 552a (LEXIS through P.L. 117-214, approved 10/19/22).

³² *Schmitt v. City of Detroit*, 395 F.3d 327, 331 (6th Cir. 2005).

³³ 42 U.S.C.S. § 290dd-2 (LEXIS through P.L. 117-214, approved 10/19/22).

³⁴ 42 CFR Part 2 (2021).

³⁵ 42 C.F.R. § 2.12(a) (2021).



FEDERAL BENEFITS LAWS

SNAP Laws

Federal SNAP law permits disclosure of SNAP applicant and participant data to persons directly connected with the administration of SNAP, federal assistance programs, or federally-assisted state programs and for the purpose of such administration. Under these federal rules, states have shared SNAP data for such uses as conducting outreach for different federal and federally-assisted benefit programs and for some research purposes.

Under federal law, a SNAP agency's state plan must include safeguards prohibiting the use or disclosure of SNAP applicant household information except to "persons directly connected with [SNAP] administration or enforcement of [SNAP statutes and regulations], federal assistance programs, or federally-assisted State programs."³⁶ This must be "only for such use or enforcement."³⁷ The data recipients must "adequately protect the information against unauthorized disclosure."³⁸ The regulations permit the SNAP agency to "inform low income households about the availability, eligibility requirements, application procedures, and benefits of the [SNAP program]."³⁹

Sharing data with third parties:

The same federal laws that allow data sharing across administering agencies permit sharing with third parties that are connected with SNAP, federal assistance programs, or federally-assisted state program administration.

WIC Laws

Federal WIC law permits the disclosure of confidential WIC applicant and participant information to persons directly connected with the administration of the WIC program who need to know the information for WIC program purposes. Under these federal rules, states have shared WIC data for WIC program purposes like WIC outreach and research.

Any WIC applicant or participant information is considered confidential.⁴⁰ The use and disclosure of the confidential applicant and participant information must be restricted to "persons directly connected with the administration or enforcement of the WIC Program whom the State agency determine have a need to know the information for WIC Program purposes."⁴¹ Although "directly connected" is not defined in WIC statutes or regulations, the law does provide guidance that the "persons" may include, but are not limited to: "personnel from its local agencies and other WIC State or local agencies; [and] persons under contract with the State agency to perform research regarding the WIC Program."⁴² Under these laws, it is more common to see other benefit programs share participant data with WIC for the purpose of analysis and outreach, as opposed to the other way around.

Sharing data with third parties:

The same laws that allow disclosure of confidential WIC information permit sharing with third parties that are directly connected with the administration of WIC and have a need to know the information for WIC program purposes.

³⁶ 42 C.F.R. § 2.12(a) (2021).

³⁷ 7 U.S.C.S. § 2020(e)(8) (2022).

³⁸ 7 C.F.R. § 272.1(c)(2) (2022).

³⁹ 7 U.S.C.S. § 2020(e)(1) (LEXIS through P.L. 117-214, approved 10/19/22).

⁴⁰ 7 C.F.R. § 246.26(d)(1) (2022).

⁴¹ 7 C.F.R. § 246.26(d)(1) (2022).

⁴² 7 C.F.R. § 246.26(d)(1) (2022).



There are no federal statutes or regulations pertaining to the disclosure of LIHEAP application information to other administering agencies.^{43,44,45} However, because the federal government provides state and local governments broad flexibility to design and implement block grant programs like LIHEAP, there are likely state-specific confidentiality and privacy laws for LIHEAP.

Sharing data with third parties:

There are no federal statutes or regulations pertaining to the disclosure of LIHEAP application information to third parties.

Federal Medicaid law permits the use and disclosure of Medicaid applicant and participant data for purposes directly connected with the administration of the Medicaid plan, including providing services for beneficiaries. HIPAA permits the disclosure of Medicaid applicant and participant data when the disclosure is part of the Medicaid agency's own healthcare operations. Under these federal rules, states have shared Medicaid participant data with other benefit programs, like SNAP and WIC, to conduct analysis and outreach that is connected to better health outcomes.

The legal rationale that states have used to support these activities relies on the well-established connection between improved nutrition and health. Under the Medicaid

regulations, an agency is allowed to use and share data to provide services for beneficiaries.⁴⁶ Agencies have concluded that providing information about nutrition benefits like SNAP and WIC that can improve health and reduce healthcare costs are permitted services under Medicaid statutes and regulations. Under HIPAA, Medicaid agencies are allowed to use and share data for its own healthcare operations.⁴⁷ Agencies have concluded that data sharing for purposes that fall within the definition of healthcare operations – including population-based activities relating to improving health or reducing healthcare costs – is permitted under HIPAA.⁴⁸ Therefore, agencies have concluded that data sharing efforts that help Medicaid recipients enroll in SNAP or WIC are permitted, as participation in those benefits leads to improved health and lowers healthcare costs.

Under federal Medicaid law, Medicaid agencies are required to safeguard the “use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan.”⁴⁹ Purposes directly related to plan administration include “providing services for beneficiaries.”⁵⁰ A Medicaid agency may “distribute materials directly related to the health and welfare of applicants and beneficiaries, such as announcements of free medical examinations, availability of surplus food, and consumer protection information.”⁵¹ Under these rules, agencies have shared Medicaid data with other programs to conduct outreach to Medicaid participants.

⁴³ 42 U.S.C.S. §§ 8621-8630 (LEXIS through P.L. 117-214, approved 10/19/22).

⁴⁴ 45 C.F.R. Part 96 Subparts A-F and H.

⁴⁵ 45 C.F.R. Part 75 (2021).

⁴⁶ 42 C.F.R. § 431.302 (2021).

⁴⁷ 45 C.F.R. § 164.506 (2021).

⁴⁸ 45 C.F.R. § 164.506 (2021).

⁴⁹ 42 U.S.C.S. § 1396a(a)(7) (LEXIS through P.L. 117-214, approved 10/19/22).

⁵⁰ 42 C.F.R. § 431.302 (2021).

⁵¹ 42 C.F.R. § 431.307(c) (2021).

To use or share Medicaid data for analysis and outreach, a Medicaid agency must also comply with HIPAA privacy rules. The Medicaid agency is considered a HIPAA “covered entity” because it administers a “health plan.”⁵² As a covered entity the Medicaid agency must comply with HIPAA privacy rules when using or disclosing data – like Medicaid participant records – that contains Protected Health Information (PHI).⁵³ PHI is defined as individually identifiable health information “that is [t]ransmitted by electronic media; [m]aintained in electronic media; or [t]ransmitted or maintained in any other form or medium.”⁵⁴ Individually identifiable health information “is a subset of health information, including demographic information collected from an individual, ... created or received by a ... health plan” and is related to a health condition of an individual, provision of healthcare, or payment for the provision of healthcare to an individual.⁵⁵ Lastly, “it identifies the individual; or ... [provides] a reasonable basis to believe the information can be used to identify the individual.”⁵⁶ The Medicaid agency may use or disclose these records containing PHI for its own healthcare operations even without consent.⁵⁷ Healthcare operations include conducting “population-based activities relating to improving health or reducing healthcare costs.”⁵⁸

Sharing data with third parties:

The same laws that allow a Medicaid agency to share participant data permits sharing with third party “business associates” for purposes directly connected with the administration of the Medicaid plan, including providing services for beneficiaries.⁵⁹ A “business associate” includes a person who “[o]n behalf of [a] covered entity... receives... protected health information for a function or activity regulated by [the HIPAA regulations]... including... administration.”⁶⁰ When disclosing protected information to a business associate, the Medicaid agency must obtain “satisfactory assurance that the business associate will appropriately safeguard the information.”⁶¹ This takes the form of a written contract⁶² commonly referred to as a Business Associate Agreement,⁶³ which third parties will need to execute with the administering agency.

UC Laws

Federal Unemployment Compensation (UC) law permits the disclosure of confidential UC information to a public official in the performance of his or her official duties.

Generally, states are required to implement methods of administration that are “reasonably calculated” [to maintain] the confidentiality of any identifying Unemployment Compensation (UC) information.⁶⁴ Confidential UC information may be disclosed to “a public official for use in the performance of his or her official duties.”⁶⁵ The disclosure must not interfere with the efficient administration of state UC law.⁶⁶ A public official is “an official, agency, or public entity within the executive branch of Federal, State, or local government who (or which) has responsibility for administering or enforcing a law, or an elected official in the Federal, State, or local government.”⁶⁷ Performance of official duties means administration of the law.⁶⁸

Sharing data with third parties:

The flexibility in UC privacy laws may enable different types of data sharing projects that utilize third parties as “agents” or “contractors” of public officials. Confidential UC data may also be shared with an agent or contractor of such public official.⁶⁹

⁵² 45 C.F.R. § 160.103 (2021).

⁵³ 45 C.F.R. § 164.502 (2021).

⁵⁴ 45 C.F.R. § 160.103 (2021).

⁵⁵ 45 C.F.R. § 160.103 (2021).

⁵⁶ 45 C.F.R. § 160.103 (2021).

⁵⁷ 45 C.F.R. § 164.506 (2021).

⁵⁸ 45 C.F.R. § 164.501 (2021).

⁵⁹ 42 U.S.C.S. § 1396a(a)(7) (LEXIS through P.L. 117-214, approved 10/19/22).

⁶⁰ 45 C.F.R. § 160.103 (2021).

⁶¹ 45 C.F.R. § 164.502 (2021).

⁶² 45 C.F.R. § 164.504 (2021).

⁶³ U.S. Department of Health & Human Services, Office for Civil Rights, “Business Associate Contracts,” June 16, 2017, [Weblink](#).

⁶⁴ 20 C.F.R. § 603.4(b) (2021).

⁶⁵ 20 C.F.R. § 603.5(e) (2021).

⁶⁶ 20 C.F.R. § 603.5 (2021).

⁶⁷ 20 C.F.R. § 603.2(d)(1) (2021).

⁶⁸ 20 C.F.R. § 603.5(e)(1) (2021).

⁶⁹ 20 C.F.R. § 603.5(f) (2021).



TELEPHONE CONSUMER PROTECTION ACT AND TEXTING OUTREACH

SMS text messaging outreach has become a powerful and comparatively inexpensive vehicle for disseminating information to individuals. It is being used by administering agencies to conduct outreach for benefits enrollment — like texting SNAP recipients to let them know they may be eligible for the Affordable Connectivity Program — as well as outreach on benefits maintenance — like texting Medicaid recipients with redetermination guidance.

The Telephone Consumer Protection Act (TCPA) is the federal law that governs phone and SMS text message solicitations.

» Data sharing projects using text messages as the outreach medium require an additional layer of legal analysis due to these federal restrictions on SMS text messaging.

The TCPA states it is “unlawful for any person...to make any call ... (other than a call made ...with the prior express consent⁷⁰ of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice— to any... cellular telephone service.”^{71,72} The Federal Communications Commission (FCC) determined that SMS text messages are subject to the same consumer protections under the TCPA as voice calls.⁷³

97%
OF U.S. ADULTS
whose income
is less than \$30,000
OWN A CELL PHONE⁷⁴

Americans today are increasingly connected to the world of digital information while “on the go” via mobile devices.

⁷⁰ Express consent is a type of consent that requires a heightened level of assent indication.

⁷¹ 47 U.S.C.S § 227 (LEXIS through P.L. 117-214, approved 10/19/22);

⁷² The FCC determined that “persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary” and thus express consent is met under the TCPA. *Aderhold v. car2go N.A. LLC*, 668 Fed. Appx. 795, 796 (citing In the Matter of RULES AND REGULATIONS IMPLEMENTING THE TELEPHONE CONSUMER PROTECTION ACT OF 1991, 7 FCC Rcd 8752, 8769 (F.C.C. September 17, 1992)).

⁷³ FCC Declaratory Ruling and Order; June 18, 2015; 30 FCC Rcd 7961 (10).

⁷⁴ Pew Research Center, “Mobile Fact Sheet,” April 7, 2021, [Weblink](#).

This has the following implications for state and local government as well as third parties that conduct SMS text outreach:

- » State government entities are exempt from the TCPA restrictions. In 2020, the FCC decided that “State government callers in the conduct of official business do not fall within the meaning of a ‘person’ in the TCPA.”⁷⁵
- » Local government and third parties that conduct texting outreach are not subject to the TCPA restrictions as long as they are not using an automatic telephone dialing system.
 - While state government callers are exempt from the TCPA restrictions, the FCC determined that federal contractors; state contractors; local government entities, including counties, cities, and towns; and local government contractors do fall within the meaning of “person” in the TCPA.⁷⁶
 - In 2021, however, the U.S. Supreme Court held that the TCPA is only applicable to entities that make calls or send texts using an “automatic telephone dialing system,”⁷⁷ defined as “a piece of equipment with the capacity both to store or produce telephone numbers to be called, using a random or sequential number generator, and to dial those numbers.”⁷⁸ Automatic telephone dialing systems are likely not used for benefits outreach since outreach is sent to the known cell phone numbers of program participants as opposed to randomly generated numbers.

EMERGING ISSUE:

Readers should be sensitive to evolving and shifting norms and practices around data that may be more stringent than what is allowed by law. For example, the trade association for the U.S. wireless communications industry, CTIA, advises that the best practice is to obtain express consent for certain types of SMS text messages.⁷⁹ In some instances, this would be a stricter interpretation of consent than what is required under the law. Texting vendors may require this heightened level of consent to do text-based outreach even though, in some instances, consent is not required under the TCPA. Agency staff will need to consider how best to navigate this emerging trend.

⁷⁵ Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, FCC 20-182 (2020).

⁷⁶ Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, FCC 20-182 (2020).

⁷⁷ Facebook, Inc. v. Duguid 141 S.Ct. 1163 (2021).

⁷⁸ Facebook, Inc. v. Duguid 141 S.Ct. 1163 (2021).

⁷⁹ CTIA, “Messaging Principles and Best Practices,” July 2019, [Weblink](#).

Consent and Equity

In the broader field of social services and government, there is consensus that people should have a say about if and how their data is used. But collecting consent can require significant effort and may collide with the desire to proactively and quickly connect individuals to critical benefits and services. These dynamics are complicated by long-standing misuses of individual data — particularly affecting people of color — which have contributed to inequitable systems. As the 2021 report, *Rising Equitable Community Data Ecosystems (ReCode)*, highlights: “people have often had little say over how data about them and their neighborhoods are collected, stored, or interpreted.”⁸⁰

The type of data sharing discussed in this Playbook is designed to help eligible individuals and families connect to and maintain critical benefits and is focused on situations where federal law permits data to be shared without individual consent. Yet questions about power and trust are inherently raised by data sharing efforts. **It is important for agencies and institutions to think critically about how they can provide broader visibility into how residents’ data are being used** while ensuring that they can easily access the services and benefits available to them.

As a provider of outreach and application support, BDT continues to evolve its understanding and implementation of best practices related to consent. **We remain committed to using data only for the purposes for which they were shared with us, and to maintaining transparency and clarity in messaging to the individuals we serve about how their data are used in their interactions with BDT.**

Emerging best practices:

- » Benefits applications at the local, state, and federal levels can include language that gives applicants the option to have their data shared for the

purpose of connecting them to additional benefits and services. The consent option should be written in clear and simple language. Proactive opt-ins may also satisfy the CTIA requirement for express consent.

- » Increasingly, organizations like Stewards of Change Institute⁸¹ are advocating for open-source, standards-compliant digital consent tools that health and human services institutions could use to request consent from individuals more easily.
- » Agencies and institutions can engage community members directly in data sharing efforts. Agencies can develop participant advisory boards to get input on data sharing policies and approaches, or directly involve residents in designing, implementing, and evaluating specific data sharing projects. Engagement takes time and effort but can lead to stronger projects and outcomes while increasing trust and understanding between government and community.
- » Agency- and administration-wide data governance policies encourage transparency and openness about when and how resident data is used. Making data policies public — and listening to community voices in developing those policies — decreases the feeling that data sharing activities are happening behind closed doors.
- » Every outreach campaign should include a simple opt-out for recipients who do not want to be contacted in the future. Agencies should have systems in place to capture that opt-out and remove that person from future outreach efforts.

For more information and additional resources, see the Consent section of Appendix III.

⁸⁰ Ginger Zielinskie, Lindsey B. Gottschalk, “Rising Equitable Community Data Ecosystems (RECoDE). The Voices We Trust: Building Equity-Centered Community Data Ecosystems That Work for Everyone,” Data.org, March 2022, [Weblink](#).

⁸¹ “Stewards of Change Institute,” Accessed November 29, 2022, [Weblink](#).

Crafting the Data Sharing Agreement

Once agencies determine that their data sharing project is permissible, the teams can begin drafting an effective legal agreement. **A DSA is a legally binding document that governs data sharing practices and serves as the common understanding between the relevant parties.** It typically says what data will be shared when, why, how, and with what protections. The DSA justifies the reason for sharing the data; explains what is being done with the data; and describes the approaches to safeguarding and protecting the data in flight, use, and disposition.

While different agencies, jurisdictions, and projects may require different legal agreements, a typical DSA includes the following elements:

- » Use case or business justification
- » Legal authority for sharing data
- » Scope of services
- » Security considerations
- » Additional terms of agreement, such as provisions for the destruction of data and Institutional Review Board authorizations (see “Ethics and Privacy” on page 55)
- » Data specifications related to the frequency of data transfer, method of transfer, file format, data range, data filters, and fields (or appended, as discussed below)
- » Duration of the agreement

It is important to include the operative legal analysis and basis for sharing benefit program data in the DSA. This documents that all parties agree with the legal analysis and allows for the continuity of current and future data sharing projects.

One way to streamline the DSA is by using a Technical Specification Document (TSD) as an appendix to the agreement. A TSD describes the data fields needed for the data matching, analysis, and outreach; the specifications of the file transfers; and the process for changing those specifications over the life of the initiative. It is a helpful reference and reduces the need to amend the entire DSA if data needs fluctuate due to operational considerations. This approach can be selected in consultation with your legal teams.

Several **data privacy and security components** must be considered and implemented into the DSA. Common elements include:

- » Identification of a data steward from each program or agency
- » Determination of when and how data should be terminated (e.g., properly deleting or erasing the data) at the end of the project and clearly defining what data deletion means
- » Identification of safe data security standards for secure storage and transmission of data
- » Defining limitations to data access: Who can and cannot access the data? Is there a procedure for adding parties to the data access list?
- » Security of data storage media: What types of storage media are permissible for storing the data and how are the media kept secure?
- » Defining data breach protocols, including who should be notified at each agency, what steps must be taken to remedy the breach, and if and how long data transfers should be suspended if a breach occurs

CASE STUDY:

Connecting Minnesotans to WIC

For many years, the Minnesota Department of Health (DOH) has **leveraged data sharing to identify and outreach to individuals** who may be adjunctively eligible for WIC but were not yet participating.

Historically, they conducted mail outreach to Medicaid participants to raise awareness about WIC, but beginning in 2021, DOH was eager to pilot text-based outreach to drive eligible households to their online WIC application. To do this, they honed their outreach list based on available data and WIC programmatic considerations to have the best chance of reaching their intended audience, enabling outreach recipients to connect to WIC as efficiently as possible.

To start, DOH established a data sharing process whereby lists of new Medicaid recipients who are highly likely eligible for WIC are sent to Minnesota WIC on a quarterly basis. The list of Medicaid recipients is matched against a list of current WIC recipients based on their name and, as available, date of birth, address, and phone. DOH then uses several criteria to refine the list, such as removing duplicate phone numbers and pregnant people under the age of 18.

DOH uses this list to conduct text-based outreach to the identified individuals, which has yielded a marked increase in online WIC applications submitted. DOH continues to refine its outreach cadence and messaging based on feedback from clients and caseworkers, but overall, has demonstrated impressive outcomes through its strategic data matching process.





SECTION 4

How to Plan, Launch, and Scale a Smooth and Efficient Data Sharing Process

While many data sharing projects start with a focus on legal authorities, data security, and privacy, there is more at play. From collaboration across agencies to pulling data from different warehouses and systems, this section is designed to help you start and sustain successful data sharing initiatives.

Imagine This:



A health and human services agency wants to increase SNAP participation by conducting outreach to current Medicaid recipients through data sharing.



It takes several weeks to scope the project and align on the legal authorities, but the SNAP legal team signs off and starts to draft an agreement to share participant data with the Medicaid team for the purposes of outreach. It quickly becomes clear that the Medicaid legal team hasn't been engaged in the process and has privacy concerns.



As a result, the project is delayed indefinitely while the two legal teams start discussions to confirm that the relevant legal authorities permit the use and sharing of both SNAP and Medicaid data for this purpose.



At the same time, the program teams consider whether the project is feasible as the data is managed by a separate vendor who also needs to be brought in on the project.



After several more months, an agreement has been reached, data is pulled, and SNAP outreach to Medicaid recipients begins. Results start coming in and with it, a new and exciting idea to improve response and enrollment rates by sending outreach in different languages.



This would require an amendment to the DSA, and teams consider starting the process over again.

This may sound familiar to anyone who has conducted data sharing activities before. While an initiative like the one above can have a tremendous impact on participants, a smoother and more efficient process is achievable. The following pages provide key steps and best practices to make the process as easy and productive as possible.



Tips for Successful Data Sharing for Benefits Analysis and Outreach

Below are best practices that can help agencies implement successful data sharing, analysis, and outreach initiatives.

Goal and Process Alignment

- » **Start by determining if and how data sharing can be used** to achieve your benefits goals; use that goal to clearly define a use case and develop a supporting legal rationale.
- » **Don't start from scratch!** Where possible, build off existing data sharing activities and agreements. If you don't have an existing DSA, the tools in the Appendix can help you get started.
- » **Expect multiple teams to review and approve the DSA.** Understanding the sign-off process will help you build a realistic project timeline.

Relationship Building and Staffing

- » **Data sharing takes time, trust, and communication.** Invest in the cross-programmatic, cross-functional relationships needed to do this work.
- » **Align early on vision and scope** with the key players — programmatic, legal, and data — from both agencies who will support the data sharing process.
- » **Find an executive champion** who will prioritize this work and galvanize teams.
- » **Budget for the staff time and capacity** needed to conduct the work throughout the project life cycle. Create a process map to understand how the data flows across teams and systems in order to determine who will be involved in the project.

Implementation and Evaluation

- » **Decide what data fields are necessary** to conduct analysis, outreach, and evaluation. This upfront planning helps legal teams understand the specific purpose for using the data and expedites legal review. It also ensures that the DSA includes the fields needed to run interventions and measure success, reducing the likelihood of needing an amendment.
- » **Include demographic data fields** in the DSA to understand disparities in access, build outreach campaigns that address those inequities, and measure for whom the intervention is or is not working.

Data and Quality Control

- » **Build a shared understanding about the definitions and formats of the data being shared** through tools like data dictionaries. This will make the sharing, matching, and analysis process significantly easier, and documentation will prevent delays in the case of staff turnover.
- » **Conduct quality control checks on the data** before you begin analysis or outreach. If initial data pulls are radically different than expected, double-check the methods used to pull the data. The process may start messy but gets easier with communication and iterative improvements!

The rest of this section includes a deeper dive into these key steps to launch, operate, sustain, and scale a data sharing project.



Aligning on Purpose and Goal

While data sharing is a powerful strategy, it is a means to an end. Start data sharing conversations by **centering the outcomes** you are hoping to achieve and then **determine if and how data sharing can help achieve those goals**.

As the “Making the Case” section outlines, data sharing can be a particularly compelling tool for agencies looking to increase participation, address retention, build holistic and efficient systems, increase equity, and more. Defining clear goals allows the project team to create a strong use case for sharing the data, which legal teams will need in order to assess the viability of the project.

“ It’s one big lesson I’ve learned: data sharing needs to be for a purpose. The data sharing itself is not the impact. It is important to focus on the thing we want to see happen as a result, and to figure out the data sharing in support of it. ”

- Philanthropy Program Officer

It’s important to find shared value for all project partners. As our interviewees shared, if one program feels it is benefitting from the project less than the other, it may prevent the initiative from getting off the ground or scaling. In a SNAP/Medicaid data sharing project, for example, SNAP can use Medicaid data as a source of outreach to increase program participation while Medicaid can benefit from reductions in healthcare costs by having participants enroll in SNAP.



Pulling Together the Team

The secret to effective data sharing projects? Relationships and trust-building.

The most consistent feedback from our interviews was that **data sharing can occur without high-end technology but is impossible without strong relationships and trust**. This is often the case when institutions explore innovative ways of doing business, and certainly the case when working with participant data that public servants have a duty to protect.

“ It’s just like anything else where you ask someone to act and think in a new way that’s different from how they have been operating for decades or more. It just takes time. There needs to be time for conversations with all of the key people involved and you need to respect that we’re asking them to think about [data sharing] differently. There needs to be time for explaining the benefits and the costs and being open and honest about the risks. Building that trust is important. ”

- **Government Health & Human Services Manager**

“ It’s actually a relationship. It’s not really just an agreement, it’s a relationship that different programs start having with each other. And then, I care about WIC, but then I also care about SNAP, the participants as well. ”

- **Government Epidemiologist**



Tips for investing in the vertical and horizontal relationships necessary for successful data sharing initiatives:

- » **Find executive champions** who prioritize data sharing! This was consistently cited as a key driver of success.
- » **Align the key teams** needed to execute data sharing agreements and activities. Too often, data sharing conversations occur in a piecemeal fashion and decisions are made without input from the necessary agencies or perspectives. BDT has found that the teams featured in the graphic below are particularly vital for data sharing for analysis and outreach. Relevant staff from both agencies should be engaged from the start to prevent delays and implementation hurdles.
- » **Identify key stakeholders by making a process map that tracks how the data will move through the system** over the life of the project and which teams are involved in pulling it, cleaning it, and sharing it. This will help uncover additional key players, like the IT staff who help transfer the data and any vendors or data management services that should be involved in the process as well.
- » **Start a working group** to define project goals, outline success criteria, and create buy-in. Investing in working groups like this is useful for individual initiatives and can help scale data sharing activities more broadly (see “Sustain and Scale” on page 45).

Key Teams:

Legal and Privacy:

Legal counsel is critical to approving any use of protected data. Legal teams from all relevant programs should be engaged from the beginning so they can understand the project and provide guidance on the key legal issues that affect the DSA. They will advise and review as the project scope is defined, write and negotiate the DSA, and may stay engaged in ongoing project governance.

Data:

These staff manage and understand the data that will be used throughout the intervention. Engaging these specialists early reduces the risk of omitting fields that are necessary for project implementation. The data staff should inform outreach decisions and provide critical guidance on data quality and interpretation.

Program and Operations:

These staff are responsible for running and administering the benefit programs. Since they are responsible for outcomes-oriented initiatives that involve data sharing – like those focused on outreach or retention – many data sharing projects originate with these teams.



Implementation Considerations that Inform the Data Needs

One particularly important aspect of executing effective DSAs is **including the exact data fields needed to conduct data matching, analysis, outreach, and evaluation.**

Responsible stewardship of protected data means agencies are inclined to share as little data as possible. Understanding the purpose of each requested element and how it benefits the intervention will inform and expedite programmatic and legal review. This planning allows for smooth implementation and prevents lengthy delays or amendment processes if additional fields are necessary.

This is also the time to explicitly build equity into this work. While the challenges of obtaining quality demographic data in human services have been well-documented,⁸² using available demographic data fields is necessary to support thoughtful and equitable data sharing.

Proactively including fields like race/ethnicity, gender, preferred language, age, disability status, veteran status, and more will allow administering agencies to assess disparities in access, design outreach that is tailored to particular populations, and understand how specific populations respond to outreach.

For a list of additional resources, see the Data Sharing & Equity section of Appendix III.

“ There are data elements that we tend not to think about until you’re analyzing the impact of a project. For example: we’ve analyzed outreach results and noticed no one in this one zip code replied to outreach. Then we dig into the data and discover commonalities among the non-responders. Our outreach letters were sent in only English, and analysis shows that the outreach likely failed to engage people because it encompasses a community that primarily speaks and reads Arabic. ”

- Health & Human Services Policy Expert

⁸² Code for America, “National Safety Net Scorecard: The Status Quo of Safety Net Assessment,” Accessed November 29, 2022, [Weblink](#).



SELECTING DATA FIELDS

Below are the data elements typically needed for data sharing projects, including demographic and geographic fields that allow agencies to integrate equity into the planning process.

Data Elements Purpose	Reason	Data Fields
Match the Files	These data are needed to match individual-level data across different programs and de-duplicate records to create the list of individuals on one program but not the other	<ul style="list-style-type: none"> • Unique identifiers such as Social Security number, Medicaid ID, participant phone number
Analyze Enrollment Trends	These data are needed to determine the size of the cross-enrollment gap across benefits and uncover geographic and/or demographic trends	<ul style="list-style-type: none"> • Demographic fields such as race, ethnicity, age, sex, etc. • Geographic fields such as zip code or county
Conduct Outreach	These data are needed to send outreach to individuals; requires an understanding of the type of outreach being sent	<ul style="list-style-type: none"> • Participant name, phone number, address, preferred language
Evaluate Outreach	These data are needed to measure the success of the outreach and its impact on specific populations and/or geographies	<ul style="list-style-type: none"> • Outreach response • Benefit enrollment status • Demographic fields such as race, ethnicity, age, sex, etc. • Geographic fields such as zip code or county

- **The method(s) of outreach will inform the data needed in your DSA.** For example, text-based outreach will require cell phone numbers, letters will require addresses, etc.
- **Consider if your outreach message requires details about the recipient.** If, for example, you want to include someone's first name in the outreach, the DSA will need to include a field for first names.
- **Your DSA should specify the preferred date range and frequency of data pulls.** If the initial match is conducted too far in advance of outreach, the outreach group may include families who have moved, changed phone numbers, are no longer eligible, or enrolled in the benefit on their own. When drafting a DSA, allowing for more frequent transfers could be helpful even if they don't always occur at the frequency stated in the contract.
- **Consider potential sensitivities in the data elements you are requesting.** For example, a person's pregnancy status or immigration status may not be something that you can or should share without good reason.
- **Outreach is a chance to build trust between government and the residents they serve.** For more resources on how to conduct outreach campaigns that engage residents and connect them to the services they need, *see the Outreach section of Appendix III.*



CONDUCTING EVALUATIONS

Evaluating outreach is a critical yet often overlooked component of the data sharing process. Start thinking about evaluation early in the process to ensure your DSA **includes the data needed to measure outcomes and success.**

Evaluating the impact of the outreach allows administering agencies to:

- Gain insight into whether the project is achieving its intended outcomes
- Assess how different populations respond to the outreach
- Provide actionable information to change and improve the intervention
- Share progress with partners, funders, and local and national audiences

To determine which data elements you need to request in the DSA, consider your evaluation questions.

Examples include:

- What is the relationship between sending outreach to Medicaid recipients and SNAP enrollment rates? Do SNAP enrollment rates vary by different demographic characteristics and/or outreach messages?
- In the state's five largest counties, do people who receive text-based outreach certify for WIC at higher rates compared to those who don't receive outreach?
- Are there differences in enrollment rates according to the type of outreach?
- Do different age groups respond similarly to text outreach?
- Do different outreach messages yield different response and/or enrollment rates?

CASE STUDY:

SNAP Outreach in South Carolina

BDT has worked with the South Carolina Department of Social Services (SCDSS) since 2015 to help senior residents access public benefits programs that help them meet their basic needs. On a monthly basis, SCDSS matches Medicaid and SNAP enrollee lists to identify those who are connected to Medicaid but not enrolled in SNAP; given similar income eligibility requirements between the programs, those identified through this matching process are highly likely eligible for SNAP. SCDSS has a DSA in place with BDT through which BDT sends outreach to South Carolinians identified in the data match to offer them assistance applying for SNAP over the phone.

20,000
ESTIMATED SNAP
ENROLLMENTS
generated by this partnership to help
SOUTH CAROLINA
SENIOR HOUSEHOLDS
afford the cost of groceries



Working with the Data

Our interviewees were clear: the logistics of accessing, sharing, and matching participant data are challenging but **lead to great outcomes**.

Data are pulled from different — often aging — systems that weren't designed to speak to each other, and the data from distinct programs and agencies are often formatted, defined, and even calculated differently. The benefit program itself might dictate key differences. For example, WIC doesn't collect Social Security numbers at all, necessitating decisions about how to match data across lists. Upfront planning and ongoing communication can ensure a successful project.

Some administering agencies have invested time, money, and effort into technology that can streamline data sharing and matching efforts. They have deployed business intelligence software to transform data into useful insights, data lakes that allow for more flexible storage of data, or a Master Person Index (MPI)⁸³ that identifies individuals across multiple systems. While this kind of technology may make the manipulation of data easier, faster, and less manual, we consistently heard that it can be done with relatively simple technology and processes.

“ You can do a lot with like a slimmed down computer in a closet. I mean, that's the cool thing about this work. It doesn't have to be fancy. ”

- Data Sharing Policy Expert

This starts with technical and programmatic experts learning about each other's data systems, infrastructure, and terminology before working with the data. The following questions can also help inform the process and timeline.

- » **Where are the data housed?** Do the data live with the agency or a vendor? Do the data from different programs live in the same or different systems?
- » **How will the data be formatted to catch duplicates in the matching process?** For example, how many digits are used to format zip codes?
- » **How will the data be transferred across systems?** Automated transfer methods reduce the number of individuals who need to interact with the data, which can be beneficial for efficiency and privacy considerations.

⁸³ For an example MPI project, see: "HHS Coalition IT Strategy, 2021-2024," p. 11, Washington Health & Human Services Coalition, Accessed November 29, 2022, [Weblink](#).



“ Make sure that the folks who are closest to the data can speak to the quirks that are going to be within that data set so that [it] is properly interpreted. Trust data owners when they say whether or not the data is going to be likely useful for outreach. ”

- Former Government Operations Administrator

When planning the data match, there are additional considerations that can lead to a successful project:

- » **Align on a unique identifier to track and match individuals across data sets.** You might need to experiment with different matching criteria to address inconsistencies, such as spelling variations in names.
- » **Discuss how the structure of program data will inform the matching process.** For example, Medicaid is an individual benefit while SNAP is a household benefit, and those differences have implications for matching and de-duplicating records.
- » **Use documentation to align on variable names, definitions, formats, and more.** Discussions about data availability, definitions, format and more will make the process faster and smoother (for a list of additional resources, see the Data Catalog/Data Dictionary section of Appendix III)
- » **Check the results of the data match before sending outreach.** Teams can run tests using files that don't contain any data and review match results to ensure that the de-duplication process went correctly. Don't worry if the first match is messy; that's to be expected!
- » **Discuss how the teams will communicate about changes** to the data throughout the project so that inevitable system changes don't lead to inaccurate data matching and outreach efforts.



Promising Practices from the Field

Our interviewees described their cross-program collaborations and the technologies they have deployed to conduct safe data sharing projects. Recent technological developments are opening new possibilities to make data sharing simpler and more secure. Below are some examples:

- » **One-way data sharing facilitates collaborations with more restrictive programs.** Agencies have different rules, regulations, or precedents for sharing participant data, and some have more restrictions than others. To work within this context, the more restrictive agency — which may be unable to share its data across program or agency lines — can receive data from another agency, run the match, and conduct outreach to those enrolled in one program but not the other.
- » **A data department or executive office can function as a “neutral third party” that receives participant data from collaborating agencies.** If it is within that internal office’s purview to handle data safely and securely, this office can run the data match and share back with the agencies the limited, relevant information needed for analysis and outreach.
- » **Application Program Interfaces (APIs) can be a key solution for limiting and controlling how data is shared for the purpose of identifying likely eligible non-participants in programs.** APIs allow one agency to automatically ask another, “is this person a program participant of yours?” and then receive a yes/no answer on a pre-defined set of attributes, thereby decreasing the need to exchange full data sets. In New Jersey,⁸⁴ for example, the WIC and SNAP administering agencies have built an API to facilitate information sharing between the programs whose data are housed separately.⁸⁵
- » **Privacy-enhancing technologies (PETs) such as the Spotlight secure analytics platform developed by Asemio and other partners in Tulsa, Oklahoma,⁸⁶ and Privacy Preserving Record Linkages (PPRL) like those examined in a project led by the CDC⁸⁷ seek to link data without exchanging PII.**
- » **Hashed data linkage is a technical method to link data while still encrypting and shielding PII.** The California Policy Lab (CPL) has piloted an exciting initiative with California state agencies to link SNAP participation and tax data using this technique.⁸⁸

⁸⁴ Jess Maneely, “Coordinating SNAP and Nutrition Supports to Reduce Child Hunger: New Jersey Spotlight, Sharing Nutrition Program Data to Raise WIC Enrollment,” American Public Human Services Association and No Kid Hungry, Accessed November 29, 2022, [Weblink](#).

⁸⁵ For more information about use of APIs in government, see: Greg Walker, “What is an API?,” 18F, April 22, 2016, [Weblink](#); Gray Brooks, “APIs in Government,” Digital.gov, April 30, 2013, [Weblink](#).

⁸⁶ Asemio, “Unlocking Insights, How Tulsa Built Momentum with Easier, Faster, and Safer Data Sharing,” Accessed November 29, 2022, [Weblink](#).

⁸⁷ U.S. Office of the Assistant Secretary for Planning and Evaluation, “Data Linkage: Evaluating Privacy Preserving Record Linkage Methodology and Augmenting the National Hospital Care Survey with Medicaid Administrative Records,” Accessed November 29, 2022, [Weblink](#).

⁸⁸ Aparna Ramesh, Evan White, Charles Davis, Samantha Fu, Jesse Rothstein, “Connecting Families to Benefits Using Linked Data: a Toolkit,” California Policy Lab, March 31, 2022, [Weblink](#).



CASE STUDY:

Enabling Privacy-enhanced Data Integration in New York City

The New York City Mayor's Office for Economic Opportunity (NYC Opportunity) supports numerous data sharing initiatives designed to give New Yorkers greater access to public benefits and services. These initiatives typically involve bringing administrative data together from two or more agencies in order to identify individuals and families most likely to be eligible for a given benefit or gaps in their services that may require immediate interventions. More often than not, the initiatives require significant legal analysis and technical effort before they can even get started.

To address these evergreen challenges, **NYC Opportunity built a privacy-enhancing data integration platform that gives a collaborating group of agencies access to a secure, automated service to match and link client records without ever having to share their entire caseloads or rosters with each other.** This platform is accessible as a web-based portal with a simple push-button interface and is intended to save time and minimize the disclosure of confidential data for the purposes of record matching. Instead of sending data files to IT staff, one or more agencies load their data separately to a secured database using the push-button interface. Based on the legal requirements governing the project, each agency or their general counsel may direct the format (e.g., individual-level, aggregated counts, merge/de-duplicated, etc.) and the destination of the integrated data set. Once done, the agencies can initiate a full purge of all data from the database and all transmission channels.

In addition to supporting benefits access, this service has also enabled new ways to support cross-agency research. Research projects often only require identifiable information so that researchers can link personal records for analysis. With NYC Opportunity's integration service, agencies with sensitive data sets can automatically crossmatch records and replace sensitive identifiers such as names, birth dates, addresses, and Social Security Number SSNs with an anonymizing research key generated by the platform. Using this key, a researcher can identify clients common across multiple data sets without ever accessing the actual identifying information about those clients.



Sustain and Scale

Whether agencies start with a small pilot or a large-scale implementation, it is important to sustain and scale data sharing efforts over time. Investments in long-term data sharing systems can build greater trust and transparency across teams, agencies, and communities while reducing the time needed for each individual project.

Considerations for sustaining and scaling data sharing efforts:

- » **Incorporate data sharing pilots into ongoing agency operations.** Once a DSA is in place, a regular process for exchanging and analyzing data and conducting outreach can become a routine activity.
- » **Share initiative results with the people that made it possible.** These outcomes remind teams of the impact of the work and why it's worth continuing. One interviewee shared, "When agencies share data with us, we strive to give them something back — whether it's information on the number of families that were reached, new research insights or even enhancements to the data they shared. In doing so, our goal is to show, in some small way, the impact that their investment of data made."
- » **Explore flexibilities in the DSA.** There may be an opportunity to focus the DSA on the overarching goal and purpose of the work while using a Technical Specification Document to address the specific data fields (see "Crafting the Data Sharing Agreement" on page 30). This allows teams to adjust outreach without lengthy amendment processes and delays. Similarly, agencies partnering with trusted third parties could streamline processes through master services agreements that provide high-level expectations around data security and usage while using individual statements of work to detail project specifics.
- » **Create and use DSA templates that different programs can adapt for their own initiatives.** Agency or statewide DSA templates can give project teams a starting point, reducing the need to start the DSA drafting process anew each time. Check out Appendix I for inspiration!
- » **Create ongoing spaces to discuss data sharing across teams.** This allows agencies to develop what one interviewee called a "one-stop shop" for data sharing conversations and enables teams to develop frameworks around collaboration, decision making, regularly used data sets, and more. This might take the form of an informal working group, an official data advisory board, or a data governance council that develops policies on safely and transparently using data.
- » **Develop documentation around commonly used data sets** so that accessing, sharing, matching, and analyzing data becomes easier over time.

For a list of additional resources, see the Data Governance section of Appendix III.

“ It's really about making sure the stuff is sustainable. I think it's great to unlock the data once, but you really need to set up a process. ”

- Data Sharing Practitioner





SECTION 5

Collaborating with Other Sectors

Engaging non-governmental sectors and partners in data sharing efforts can be a powerful way to improve the benefits system. Healthcare and higher education institutions and community outreach partners are particularly well-positioned to reach individuals who are likely eligible for benefits. Research partners can build evidence regarding the connections between benefits participation and health, education, and economic outcomes. This section highlights the role these sectors can play in advancing benefits access, and key considerations for engaging in data sharing efforts, often in partnership with government.

BDT has significant experience working with and across these sectors. Reach out to us at partnerships@bdtrust.org with any sector-specific questions or to explore opportunities for partnership.

Healthcare

From helping people manage chronic conditions⁸⁹ to reducing hospitalizations,⁹⁰ there is strong evidence that access to benefits like SNAP and WIC improves health outcomes and reduces spending on avoidable care.⁹¹

There is a significant incentive for administering agencies and healthcare institutions — particularly those bearing the burden of healthcare costs — to **address the social drivers of health by helping participants enroll in public benefits**. Data sharing between government and healthcare can be a powerful tool to support this kind of SDOH intervention.

Certain health insurers like Medicaid managed care organizations (MCOs), Medicare Advantage plans, and Individual Marketplace plans cover a patient population that is likely eligible for additional benefits. Some plans are incentivized to invest in efforts that improve health outcomes and reduce spending: a significant portion of their revenue is from capitated payments — a fixed amount of money per patient — received through risk-sharing contracts with Medicare and state Medicaid agencies. As part of these contracts, some states require MCOs to help with their members' social needs, like connecting members to social services and benefits.

This is where data sharing comes in: when health plans receive participation data from government agencies, it allows them to **understand which patients are not currently enrolled in benefits like SNAP, WIC, and LIHEAP, and build effective screening, outreach, and enrollment interventions**.

90%*
OF MEDICAID HEALTH PLANS
say improved data sharing between
government agencies and health plans would
HELP HEALTH PLANS
ADDRESS SDOH

*According to a 2022 survey by the Institute for Medicaid Innovation⁹²

When administering agencies and health payers share timely and specific benefit participation data, they can:

- » Know which plan members are receiving benefits, allowing them to conduct outreach to those who are not enrolled.
- » Report outcomes that help the state evaluate MCO efforts to connect members to social services.
- » Assist with Medicaid coverage and benefit maintenance by sending outreach and reminders about how to complete the required recertification process.
- » Extend the reach of critical support programs, thereby increasing the efficiency of public dollars.
- » Evaluate the impact of benefits assistance campaigns on member health status, care utilization, and costs.

⁸⁹ Hilary Hoynes, Diana Whitmore Schanzenbach, Douglas Almond, "Long-Run Impacts of Childhood Access to the Safety Net," *American Economic Review* (Vol. 106, No.4), April 16, 2022, [Weblink](#).

⁹⁰ Benefits Data Trust, "Seniors and SNAP," 2022, [Weblink](#).

⁹¹ Seth A. Berkowitz, Deepak Palakshappa, Joseph Rigdon, Hilary Seligman, Sanjay Basu, "Supplemental Nutrition Assistance Program Participation and Health Care Use in Older Adults," *Annals of Internal Medicine*, December 2021, [Weblink](#).

⁹² Institute for Medicaid Innovation, "2022 Annual Medicaid MCO Survey Social Determinants of Health (SDOH)," 2022, [Weblink](#).



CASE STUDY:

Data Sharing with Pennsylvania MCOs

In 2021, the Pennsylvania Department of Human Services began to share individual-level SNAP participation data with all MCOs in Pennsylvania. This gives MCOs better insight into whether each of their members is enrolled in a critical public benefit and has the potential to influence how MCOs include benefits access in planning their SDOH efforts. The process will also enhance MCOs' ability to work with non-profits, enabling the plan and their community partners to focus outreach on people who are likely eligible and not accessing SNAP. Health plans and administering agencies can enter into DSAs to enable this work and develop a shared understanding of the benefit enrollment data. Increasingly, states across the country are working with MCOs to implement similar methods, demonstrating the effectiveness of data sharing strategies to address the social drivers of health.

Administering agencies and healthcare stakeholders can consider different data sharing arrangements to help meet their goals. Some options include:

- » **Systematic list transfers:** As illustrated above, state agencies can share program data directly with health service organizations such as Medicaid managed care plans. Data from the state could be sent with daily or monthly eligibility files ("834 files") to MCOs, or via separate files.
- » **Healthcare systems of record:** Making SNAP and WIC data available to healthcare teams using various systems of record (e.g., electronic medical records, case management tools) could enrich their screening and referral activities. Including benefit participation information can provide clinical teams with a fuller picture of the medical and nonmedical interventions patients are receiving and allow them to provide patients with additional assistance. For example, if a patient is screened as food-insecure and is not currently enrolled in SNAP, then a healthcare team could help them complete an application or refer them to a community-based organization for assistance.

For Example:

Rhode Island's KIDSNET is a child health information system that connects families, pediatric providers, and public health programs — and includes WIC participation status.⁹³ This system enables pediatric providers to screen patients for WIC participation in the same place where they access state immunization data. Examples like this point towards a future where healthcare providers can easily track and act upon benefits participation data.

⁹³ State of Rhode Island Department of Health, "KIDSNET," Accessed November 29, 2022, [Weblink](#).





Health information exchanges (HIEs): HIEs bring together data from many sources, including health systems, plans, and other care services. Administering agencies can directly send data to HIEs, which healthcare organizations can use to focus their care management efforts. Many HIEs already prioritize the collection of “social risk factor” data elements; this data can and should include enrollment status in benefits programs. BDT has built an innovative partnership with the Pennsylvania Department of Aging and the Greater Philadelphia HealthShare Exchange that uses HIE’s real-time patient data to identify seniors who had been admitted, transferred, or discharged from hospitals to connect them to prescription assistance and other critical benefits.⁹⁴

Organizing and transmitting data between agencies and their healthcare partners requires significant collaboration, including education about benefit programs and discussions about data usefulness and accessibility. Both partners will have legal and security considerations regarding what data can be shared for what purpose as well as operational considerations about how often that data can be shared. Implementation will be an iterative process and can be expedited through task forces, collaboration with HIEs, and starting with simple data elements for basic analysis and outreach. Data sharing efforts can grow to explore more stratified metrics and outcomes evaluations over time.

⁹⁴ Caiti Roth-Eisenberg, Elisa Zygmunt, “Health exchange data: A powerful tool to meet patients’ needs,” Benefits Data Trust, November 7, 2019, [Weblink](#).



Higher Education

Increasingly, today's students are parents or caregivers, the first in their families to go to college, financially independent, and/or seeking retraining for a new career. Juggling responsibilities at school and home, millions of students struggle each year to afford both college and basic needs such as food, broadband, childcare, housing, and healthcare. Benefits like SNAP, Medicaid, WIC, and broadband assistance can help students meet basic needs and stay enrolled in college, but these programs are underutilized.

2 MILLION
COLLEGE STUDENTS
ELIGIBLE BUT NOT
PARTICIPATING IN SNAP

**estimated by the Government Accountability
Office before the pandemic⁹⁵**

A gap that likely exists because both students and their institutions may not know they are eligible to apply.

Leveraging data sharing is one way that institutions of higher education (IHEs) can help connect students to benefits.

By instituting DSAs with administering agencies, local health departments, or community outreach partners, colleges and universities can:

- » Understand which benefits their students may already be receiving
- » Identify students who may be eligible for benefits but not enrolled
- » Share information with third parties that can administer outreach and support for students to apply for benefits

Additionally, IHEs can use data to internally identify students who are likely eligible for benefits to inform outreach to those students, with or without sharing information with a third party. BDT will be releasing a toolkit in early 2023 to assist colleges and universities in using data elements they already hold to identify students who are likely eligible for benefits.⁹⁶

⁹⁵ U.S. Government Accountability Office, "Food Insecurity: Better Information Could Help Eligible College Students Access Federal Food Assistance Benefits," December 21, 2018, [Weblink](#).

⁹⁶ Trooper Sanders, "Helping Students Secure Basic Needs," Benefits Data Trust, September 27, 2022, [Weblink](#).



Privacy and Legal Considerations

IHEs can leverage the data they hold to improve student access to benefits while staying in compliance with their obligations to the Family Educational Rights and Privacy Act (FERPA), which protects the use of a student’s educational records. Since 2019, institutions have had the authority to share FAFSA data — with a student’s written consent — with an organization that assists a college student in applying for and receiving federal, state, local, or tribal assistance that helps offset the cost of attendance.⁹⁷ Written consent must be “signed and dated” and it must specify the records that may be disclosed; state the purpose of the disclosure; and identify the party or class of parties to whom the disclosure may be made.⁹⁸

In January 2022, the U.S. Department of Education released a Dear Colleague Letter that reminded IHEs of this authority and articulated the ways FAFSA data can aid in the administration of several federal benefits.⁹⁹

Collecting Written Consent

Given the requirements to obtain written consent from students prior to sharing FAFSA data, building consent collection into IHE processes and forms can set up IHEs to enter data sharing agreements. IHEs might consider building a consent question into one or more forms that reach their students. Some suggested places to collect student consent are:

- » Admissions or enrollment applications
- » Class registration forms
- » Financial aid award acceptance forms
- » Referral intake forms (e.g., resource navigators, case management)
- » Other forms that are commonly completed by students with financial need or basic needs insecurity (e.g., intake form at a campus food pantry or applications for emergency aid)

⁹⁷ Department of Defense and Labor, Health and Human Services, and Education Appropriations Act, 2019 and Continuing Appropriations Act, 2019, Division B, Title III, Sec. 312.

⁹⁸ 34 C.F.R. 99.30 (2021).

⁹⁹ U.S. Department of Education, Office of Federal Student Aid, “(GEN-22-02) Use of FAFSA Data to Administer Federal Programs,” January 20, 2022, [Weblink](#).



In drafting a consent question to integrate into forms students complete, consider:

- » Clear, direct language about how data will be used and what data might be shared
- » Assurances that students will not be penalized if they opt not to share their data
- » Behavioral science principles that can motivate individuals to take action

The language below may be adapted to your institution's needs for collecting consent.

Example:

ABC College doesn't want you to miss out on assistance paying for food, internet, or other basic needs to help you succeed in college. If you enroll, do you allow ABC College to share your contact information with [partner organization] to help you claim financial assistance for which you may be eligible?

If you choose "yes," you may receive text outreach to advise you on next steps and may opt out of messages at any time.

If you choose "no," your enrollment at the college will not be affected.

CASE STUDY:

Using Data to Help Students Thrive

Since 2021, the Community College of Allegheny County (CCAC) has partnered with the Allegheny County Department of Human Services (ACDHS) to streamline student referrals and services between the two organizations. A DSA allows for CCAC's Resource Navigators to access ACDHS's data system to see which ACDHS services students have already accessed, such as housing assistance or receipt of SNAP benefits. In turn, ACDHS regularly receives data for students enrolled at CCAC, which assists ACDHS staff and related community partners in coordinating care for current ACDHS clients. This closed-loop referral allows for CCAC and ACDHS to collaborate and provide timely and relevant support to students.



Community Outreach Partners

Sharing data with external organizations like application assisters, social service providers, or CBOs can be a highly valuable strategy in the effort to improve benefits access. There are many reasons why government as well as higher education and healthcare institutions may want to share data with community outreach partners to connect residents to benefits.

A community outreach partner may...

- » **be a trusted intermediary with strong relationships in the community.** Residents might be more likely to respond to messages from a community partner than a government agency, and the community partner might be able to provide tailored application assistance.
- » **have the capacity or flexibility to send outreach more quickly than a government agency.** This may be ideal if an agency or institution is interested in testing a new approach but is hindered by staff availability or competing priorities.
- » **have the technology infrastructure needed to send outreach.** While more government agencies are investing in text messaging platforms, those without access could work with an entity that does and is well-versed in deploying texting initiatives.

Institutions that want to share data with a community outreach partner will need to ensure the organization has adequate data security systems in place. **Agencies that regularly work with community outreach partners should create clear standards about how and when they share data,** so that those organizations are prepared to meet required security and privacy standards. Community outreach partners seeking to access data from administering agencies and institutions will need to make a case as to why they should receive and use the data and provide extensive information about the data security protocols they have in place. For more information on how the law applies to sharing data with third parties, see the “Federal Benefits Laws” analysis that begins on page 24.

Sharing this data can lead to incredibly positive outcomes for institutions, agencies, organizations, and — most importantly — the communities they all serve.



CASE STUDY:

Addressing Economic Challenges

During the Great Recession and again during the peak of the COVID-19 pandemic, BDT partnered with the Pennsylvania Department of Labor & Industries (L&I) and Department of Human Services (DHS) to connect residents to key benefits while experiencing an economic shock. From 2010-2014, BDT worked with both agencies to identify individuals across the state who had recently exhausted or were ineligible for UC and who were not currently enrolled in SNAP. This effort led to the submission of over 17,000 SNAP applications; it helped individuals and families put food on the table and generated nearly \$40 million in economic activity during the years of outreach.

In 2021, BDT, DHS, and L&I relaunched a similar partnership to support those who began receiving UC as a result of job losses in the early stages of the COVID-19 pandemic and whose benefits were about to expire. BDT outreached to over 106,000 people through various mediums and with different calls to action. Our research, which included a smaller subset of outreach recipients, showed that individuals who received any form of outreach from BDT enrolled in SNAP at significantly higher rates than those who didn't. These efforts have demonstrated the power of data sharing across UC and human service systems, and the importance of connecting residents to stabilizing benefits in economically challenging times.

Research

Administering agencies delving into data sharing for analysis and outreach may have key questions they are hoping to answer, including:

- » Which outreach strategies are most effective?
- » Do different strategies work better for people based on their demographic characteristics?
- » What is the relationship between receiving benefits and health, economic, and education outcomes?

Engaging in research yields insights that speak to these questions and many others. **Research studies can generate important information that can improve benefits systems, better serve participants, and help fuel a deeper understanding of benefits** for practitioners and administrators across the country.

While some agencies have the in-house expertise and capacity to conduct evaluations (see "Conducting Evaluations" on page 40), more rigorous research projects and study designs may benefit from data sharing partnerships with third-party researchers and evaluators. Third-party researchers can lend needed expertise and capacity to design and execute studies and can often secure funding to support the work. Administering agencies frequently have important questions that require investigation, as well as access to data that is vital for answering these questions.

Agencies may have concerns about dedicating time to research initiatives or sharing individual-level data with third parties for research purposes. But thoughtful conversations that find shared value between the parties can lead to research that delivers important outcomes for residents and helps inform future directions.



Ethics and Privacy

Most research is governed by regulations outlined by the U.S. Department of Health and Human Services (HHS) to ensure ethical standards are met and that research subjects are protected. Third-party researchers, particularly those in academic institutions, need to submit a research plan to an Institutional Review Board (IRB) — a group that has been formally designated to ensure that appropriate steps are taken to protect the rights and welfare of people participating in research, and to weigh the benefits against the costs and risks of the proposed research.¹⁰⁰ The IRB process ensures that research is being conducted according to laws and best practices.

Typically, researchers need access to individual-level data to conduct their analysis. While agencies may be reluctant to share this information, the data do not need to be individually identifiable. **Often, one party can generate a unique identifier that can be used to link different data sets to support analysis and all PII will be removed from the file.** This way, researchers cannot identify individuals from the data set and the privacy of individuals is protected (see page 44 for an example of this concept). Furthermore, when affiliated with a university or large research organization, researchers typically have the infrastructure and governance in place to uphold the highest standards of data security.

Initial conversations between third-party researchers and administering agencies take place over the course of weeks or months as the parties align on interests, goals, and research questions. Then the planning around study design, data sources, and data sharing begins.

Considerations for a Research Process

- » **The data needed for a study may be housed by separate offices** (for example, Medicaid claims data and SNAP enrollment information) and each office will need to approve the use of data for research purposes. In some cases, the agency may match the data across different offices, and in others it may be up to the research team to match, using an auto-generated research ID.
- » **Researchers are often interested in using a randomly assigned control group**, which requires setting aside a group of individuals at random who will not receive the intervention. This allows for an unbiased comparison of outcomes between those who received the intervention and those who did not. While withholding an intervention may give some agencies pause, this can often be addressed by delivering the intervention to the control group after the study is complete. In cases where it cannot, the potential long-term benefits can be weighed against potential risks posed to individuals in the control group. An IRB can play an important role in informing these decisions.
- » **Discuss final deliverables and expectations for disseminating findings early in the process.** Academic researchers are often interested in publishing findings in a peer-reviewed journal; administering agencies can request that researchers not reveal the name of the jurisdiction in any publications. There are many other opportunities to share research that may be more accessible to a practitioner audience through mediums like blog posts, conferences, and more. Sharing findings can help inform future research and contribute to a larger body of evidence about benefits access.

¹⁰⁰ 44 C.F.R. § 46, U.S. Department of Health & Human Services, March 10, 2021, [Weblink](#).





Appendix

Throughout our interviews, we heard a hunger for data sharing tools and resources. Practitioners are eager to see data sharing examples, templates, sample DSAs, data governance models, and more. We have compiled several of these resources in the following pages and hope they support and encourage efforts across the country. If you have a resource that you would like to share with us, please reach out to us at partnerships@bdtrust.org and we will incorporate these resources into our documents moving forward.

This section includes the following:

- Appendix I: Data Sharing Agreement Shells
- Appendix II: Sample Data Sharing Agreements
- Appendix III: Additional Resources



Appendix I: Data Sharing Agreement Shells

This appendix includes one-way and multi-way DSA shells to illustrate the common components of these legal agreements. The [downloadable version of these shells](#) can be customized for each agency and project. Throughout the document, there are plain-language explanations and directions in red text to guide you through the various sections of the DSA.



One-Way Data Sharing Agreement (DSA) Shell

[[Primary Entity]] ([[Benefit Program]]) –
[[Secondary Entity 2]] ([[Benefit Program]])

Note: This tool is a data sharing agreement (DSA) shell that is meant to help you understand the common components of a DSA involving one-way data sharing from one benefit program to another. In this shell, the Primary Agency is receiving the Secondary Agency's program data for the purposes of outreach. For example, if Medicaid is sharing its participant data with SNAP for the purpose of SNAP outreach, SNAP is the Primary Agency and Medicaid is the Secondary Agency.

The downloadable version of this shell, available [here](#), can be customized using information specific to your outreach project. **Throughout the document, there are plain-language explanations and directions in red text to guide you through the various sections of the DSA, which you can delete once you are finished.**

Adapting this document will require collaboration with key stakeholders, especially your legal, data, privacy, and security teams. Because your circumstances may differ from this example, your team may need to further customize your DSA.

Article I: Business Justification and Scope of Services

Primary Agency

Entity: [Agency and/or Division receiving data. Identified as **Primary Entity** in remainder of template]

Agency Data Steward: [Name of primary person responsible for agency data]

Steward's Title: [Data steward's title]

Address: [Data steward's work address]

Phone Number: [Data steward's work phone number]

Email: [Data steward's work email]

Secondary Agency

Entity: [Agency or division with custody of program data that is the basis of outreach. Identified as **Secondary Entity** in remainder of template]

Secondary Agency Data Steward: [Name of person who will be responsible for agency data]

Steward's Title: [Data Steward's title]

Address: [Data Steward's work address]

Phone Number: [Data Steward's work phone number]

Email: [Data Steward's work email]

This agreement is compliant with [relevant controls]

Business Justification:

[If applicable: [Primary Entity] adheres to the principle of least privilege, meaning that recipients of data and information should receive no more information than is absolutely required in order to complete an assigned project, job, task, or responsibility.]

The purpose of this DSA is to create an agreement between [Primary Entity] and [Secondary Entity] to provide outreach to families who are receiving [Secondary Entity Benefit(s)], e.g., Medicaid, SNAP, etc.] and who are likely eligible for but not enrolled in [Outreach Program, e.g., Medicaid, SNAP, etc.] in order to increase utilization of program services.

To this end, the Agreement provides conditions and safeguards for a limited exchange of Personally Identifiable Information (PII) between the parties while protecting the confidentiality of [Primary Entity and Secondary Entity] members, applicants, and participants, consistent with requirements of federal and state law.

[Specific legal analysis of applicable data sharing and confidentiality law.] *For more on the legal analysis related to sharing particular program data, see “Section 3: The Building Blocks of Data Sharing” of Data Sharing to Build Effective and Efficient Benefits Systems.*

Scope of Services:

Tip: It may be helpful to specify in the data sharing agreement or an accompanying document how the data sharing process will be initiated. Are there processes for requesting data reports from agency systems? If yes, what are they?

[Primary Entity] agrees to:

- Utilize the data provided by [Secondary Entity] only for the purpose outlined in the business justification (above).
- Match the data provided by [Secondary Entity] against current databases of [Primary Entity Benefit(s)] participants to identify those individuals who are enrolled in these services but not in [Primary Entity Benefit(s)], as outlined in **Article III, Section 1.**
Tip: This model DSA assumes the Primary Entity will conduct the match, but in some cases it may instead be the Secondary Entity. Therefore, this section may or may not need to be adjusted for your initiative.
- De-duplicate the lists generated during matching, add phone numbers and system-generated household IDs, and apply “likely to be eligible for [Primary Entity Benefit(s)]” business rules to the resulting dataset.
- [Add other terms and conditions to articulate and facilitate data sharing.]

[Secondary Entity] agrees to:

- Provide an estimate of the time required to fulfill the request within five business days of this agreement being finalized.
- Provide the identifiable data outlined in **Article III** to [Primary Entity].

This agreement is compliant with [relevant controls]

- [Add other terms and conditions to articulate and facilitate data sharing.]

Tip: What additional information or process changes would enable easier, more effective data sharing?

Article II: Term Agreement

The terms and conditions contained herein shall be binding once this Agreement is signed by all parties.

- 1) [Secondary Entity] does not guarantee the completeness or accuracy of provided data.
- 2) This agreement shall continue to be in force until all parties agree to its termination under the provisions in **Article V**.
- 3) Institutional Review Board (IRB) authorization [is/is not] required. If IRB authorization is required, data will not be transferred until and unless such authorization is obtained. Information on [Primary Entity] IRB can be found at: [website link or other location].
- 4) Upon termination of this agreement, [Primary Entity] must destroy, delete, or otherwise permanently remove all copies of the data transferred by [Secondary Entity], whether in electronic or physical format. This includes copies in raw form to which additional data have been added, but does not include aggregated output, final analyses, or any reports, charts, graphs, etc., resulting from the analyzed data. [Primary Entity] must provide written proof of destruction to [Secondary Entity] within [specified time period] of termination.
- 5) This agreement shall be reviewed annually and as required to satisfy changing requirements.
- 6) There is no cost associated with this agreement.

Article III: Data Specification

[Secondary Entity] will supply the following data to [Primary Entity]:

Tip: The purpose of this section is to set up the data transfer from Secondary Entity to Primary Entity to create a Primary Entity Benefit outreach list.

<p>Frequency: <i>Tip: How often will data be shared?</i></p>	<p>[Describe how often (and how many times) data will be exchanged, e.g., quarterly, four times]</p>
<p>Method of Transfer: <i>Tip: How will data be shared securely?</i></p>	<p>[Describe how data will be exchanged between entities, e.g., SFTP]</p>
<p>File Format: <i>Tip: Where are the data housed and in what format?</i></p>	<p>[Describe the format in which data will be exchanged, e.g., CSV]</p>
<p>Date Range:</p>	<p>[Describe any time-based filters to apply to the data, if applicable, e.g., data added in the previous quarter]</p>

This agreement is compliant with [relevant controls]

<i>Tip: What date range will the data cover?</i>	
Other Filters:	[Describe any additional filters to be applied to the data, e.g., children under 5]

<u>Element – Short Name</u>	<u>Element – Long Name</u>	<u>Format</u>
<i>Tip: Which data elements will be shared? For ideas on data needed to conduct the data match, send outreach, and evaluate the project, see “Selecting Data Fields” on page 39 of Data Sharing to Build Effective and Efficient Benefits Systems. You can also make this into a Technical Specification Document that is appended to the DSA.</i>		
EXAMPLE: BIRTH_DATE	Participant’s Date of Birth	Char(8) MMDDYYYY

Article IV: General Provisions

Nothing in this Agreement shall be construed as authority for any party to make commitments that will bind any other party beyond **Article I** contained herein.

All parties agree to:

- 1) Adhere to all security standards as for secure data storage and transmission as expressed in [relevant data security standard, e.g. SOC 2 – Type II certification].
- 2) Prohibit and prevent re-disclosure of any other party’s data to any entity not covered by this agreement.
- 3) Prohibit and prevent storage of any party’s data on mobile or portable data storage media without:
 - a) Documented business necessity approved in writing by the data stewards of all parties.
 - b) Documentation that all data storage media are physically and logically secured and acknowledged by an Information Security Officer from each party.

This agreement is compliant with [relevant controls]

- 4) Provide immediate notification to all other parties if a breach, loss, theft, or other compromise of sensitive electronic or physical data is suspected within 24 hours of discovery. Notification contacts are as follows:
 - a) [Primary Entity], [Contact Name], [Contact Title], [Contact Phone Number], [Contact Email]
 - b) [Secondary Entity], [Contact Name], [Contact Title], [Contact Phone Number], [Contact Email]

Article V: Termination

Either party may opt out of this Agreement without cause upon [Number (#)] days written notice to the other party.

Either party may opt out of this Agreement immediately, via written notice, upon discovery of a data breach suffered by either party.

Either party may suspend its involvement in this Agreement immediately upon discovery of a data breach suffered internally. Suspension of this Agreement shall not last more than [Number (#)] days and this Agreement must either be reinstated or terminated per the terms of this Agreement by the end of that period. Suspension and reinstatement/termination must include written notice to the other party.

This Agreement shall remain in full effect until replaced by a subsequent Agreement, unless sooner terminated as provided herein.

This Agreement shall automatically be terminated upon:

1. Fulfillment of all terms; or
2. When superseded; or
3. After a period of [Number (#)] years.

This Agreement [may/may not] be re-negotiated or renewed upon termination, following an appropriate review of all terms and conditions.

Article VI: Integration, Modification, and Assignment

This document represents the entire Agreement between both parties. Any modification of these terms must be in writing and signed by both parties. This agreement shall be interpreted in accordance with the laws of the [State]. Signed copies of this agreement, and any modifications, shall be kept on file with [Primary Entity and/or Secondary Entity] Office of Information Management.

#The remainder of this page is intentionally left blank#

Signatures

The undersigned hereby acknowledge and accept the responsibilities, terms, and conditions laid out in this Data Sharing Agreement:

NAME | Date
[Primary Entity]
TITLE

NAME | Date
[Primary Entity]
TITLE

NAME | Date
[Secondary Entity]
TITLE

NAME | Date
[Secondary Entity]
Title

#End of Document#

Appendices:

- a. Project Documentation

Multi-way Data Sharing Agreement (DSA) Shell

[[Primary Entity]] ([[Benefit Program]]) –
[[Secondary Entity 2]] ([[Benefit Program]]) – [[Third Party Entity]]

NOTE: This tool is a data sharing agreement (DSA) shell that is meant to help you understand the common components of a DSA involving multi-way data sharing between benefit agencies and a third party. In this shell, the Primary Agency is receiving the Secondary Agency's program data to conduct a data match, and then sharing the results of that data with the Third Party Entity. For example, if Medicaid is sharing its participant data with SNAP for the purposes of SNAP outreach and a texting vendor receives the data for outreach, SNAP is the Primary Agency, Medicaid is the Secondary Agency, and the texting vendor is the Third Party Entity.

The downloadable version of this shell, available [here](#), can be customized using information specific to your outreach project. **Throughout the document, there are plain-language explanations and directions in red text to guide you through the various sections of the DSA, which you can delete once you are finished.**

Adapting this document will require collaboration with key stakeholders, especially your legal, data, privacy, and security teams. Because your circumstances may differ from this example, your team may need to further customize your DSA.

Article I: Business Justification and Scope of Services

Primary Agency

Entity: [Agency and/or Division receiving data. Identified as **Primary Entity** in remainder of template]
Agency Data Steward: [Name of primary person responsible for agency data]
Steward's Title: [Data steward's title]
Address: [Data steward's work address]
Phone Number: [Data steward's work phone number]
Email: [Data steward's work email]

Secondary Agency

Entity: [Agency and/or Division with custody of program data that is the basis of outreach. Identified as **Secondary Entity** in remainder of template]
Secondary Agency Data Steward: [Name of primary person who will be responsible for the data]
Steward's Title: [Data Steward's title]
Address: [Data Steward's work address]
Phone Number: [Data Steward's work phone number]
Email: [Data Steward's work email]

This agreement is compliant with [relevant controls]

Recipient Entity: [Third party such as contractor(s) and/or other entities involved in the project that will need access to the data, such as vendors of outreach applications, independent evaluators, etc. Identified as **Third Party Entity** in remainder of template]

Authorized Recipient: [Name of person with third party entity who will be responsible for shared data]

Title: [Authorized recipient's title]

Address: [Authorized recipient's work address]

Phone Number: [Authorized recipient's work phone number]

Email: [Authorized recipient's work email]

Tip: For easy reference in completing the rest of this template, list out the Entities here:

Primary Entity: _____

Secondary Entity: _____

Third Party Entity: _____

Business Justification:

[If applicable: [Primary Entity] adheres to the principle of least privilege, meaning that recipients of data and information should receive no more information than is absolutely required in order to complete an assigned project, job, task, or responsibility.]

The purpose of this DSA is to create an agreement between [Primary Entity], [Secondary Entity], and [Third Party Entity] to provide outreach to families who are receiving [Secondary Entity Benefit(s)] and who are likely eligible for but not enrolled in [Primary Entity Benefit(s)] in order to increase utilization of program services.

[Third Party Entity] will perform outreach activities to those households identified as not participating, but which are eligible to participate, in [Primary Entity Benefit(s)]. **Tip:** This language establishes that outreach will be conducted through a third party for Primary Entity Benefit(s) outreach. This may or may not be applicable to your initiative.

To this end, the Agreement provides conditions and safeguards for a limited exchange of Personally Identifiable Information (PII) between the parties while protecting the confidentiality of [Primary Entity Benefit(s)] and Secondary Entity Benefit(s) members, applicants, and participants, consistent with requirements of federal and state law.

[Specific legal analysis of applicable data sharing and confidentiality law.] For more on the legal analysis related to sharing particular program data, see "Section 3: The Building Blocks of Data Sharing" of Data Sharing to Build Effective and Efficient Benefits Systems.

This agreement is compliant with [relevant controls]

Scope of Services:

Tip: It may be helpful to specify in the data sharing agreement or an accompanying document how the data share will be initiated. Are there processes for requesting data reports from agency systems? If yes, what are they?

[Primary Entity] agrees to:

- Utilize the data provided by [Secondary Entity] only for the purpose outlined in the business justification (above).
- Match the data provided by [Secondary Entity] against current databases of [Primary Entity Benefit(s)] participants to identify those individuals who are enrolled in these services but not in [Primary Entity Benefit(s)], as outlined in **Article III, Section 1.**
Tip: This model DSA assumes the Primary Entity will conduct the match, but in some cases it may instead be the Secondary Entity. Therefore, this section may or may not need to be adjusted for your initiative.
- De-duplicate the lists generated during matching, add phone numbers and system-generated household IDs, and apply “likely to be eligible for [Primary Entity Benefit(s)]” business rules to the resulting dataset.
- Transmit the resulting de-identified dataset of households and phone numbers to [Third Party Entity], as outlined in **Article III, Section 2.**
- Transmit an identifiable dataset containing individuals, phone numbers, and addresses to [Secondary Entity] as outlined in **Article III, Section 3.**
- [Add other terms and conditions to articulate and facilitate data sharing].

[Secondary Entity] agrees to:

- Provide an estimate of the time required to fulfill the request within five business days of this agreement being finalized.
- Provide the identifiable data outlined in **Article III, Section 1** to [Primary Entity].
- Use datasets received from [Primary Entity] and [Third Party Entity] to analyze the effectiveness of [Third Party Entity’s] outreach program.
- [Add other terms and conditions to articulate and facilitate data sharing.]
Tip: What additional information or process changes would enable easier, more effective data sharing?

[Third Party Entity] agrees to:

- Not identify, or attempt to identify, any de-identified data received from [Primary Entity] or [Secondary Entity] during this project.
- Utilize the received data only for the outreach program as outlined in supporting material (see Appendix A).
- Deliver results to [Primary Entity] and [Secondary Entity] as outlined in **Article III, Section 4.**
- [Add additional terms and conditions to articulate and facilitate data sharing.]

This agreement is compliant with [relevant controls]

Article II: Term Agreement

The terms and conditions contained herein shall be binding once this Agreement is signed by all parties.

- 1) [Secondary Entity] does not guarantee the completeness or accuracy of provided data.
- 2) This agreement shall continue to be in force until all parties agree to its termination under the provisions in **Article V**.
- 3) Institutional Review Board (IRB) authorization [is/is not] required. If IRB authorization is required, data will not be transferred to [Primary Entity] until and unless such authorization is obtained. Information on the [Primary Entity] IRB can be found at: [website link or other location].
- 4) Upon termination of this agreement, [Primary Entity] must destroy, delete, or otherwise permanently remove all copies of the data transferred by [Secondary Entity], whether in electronic or physical format. This includes copies in raw form to which additional data have been added, but does not include aggregated output, final analyses, or any reports, charts, graphs, etc. resulting from the analyzed data. [Primary Entity] must provide written proof of destruction to [Secondary Entity] within [specified time period] of termination.
- 5) Upon termination of this agreement, [Third Party Entity] must destroy, delete, or otherwise permanently remove all copies of the data transferred by [Primary Entity], whether in electronic or physical format. This includes copies in raw form to which additional data have been added, but does not include aggregated output, final analyses, or any reports, charts, graphs, etc., resulting from the analyzed data. [Third Party Entity] must provide written proof of destruction to [Primary Entity] within [specified time period] of termination.
- 6) This agreement shall be reviewed annually and as required to satisfy changing requirements.
- 7) There is no cost associated with this agreement.

Article III: Data Specification

Section 1: [Secondary Entity] will supply the following data to [Primary Entity]:

Tip: The purpose of this section is to allow the Primary Entity to match its data against the Secondary Entity's data to create a Primary Entity Benefit outreach list.

Frequency: <i>Tip: How often will data be shared?</i>	[Describe how often (and how many times) data will be exchanged, e.g., quarterly, four times]
Method of Transfer: <i>Tip: How will data be shared securely?</i>	[Describe how data will be exchanged between entities, e.g., SFTP]
File Format: <i>Tip: Where are the data housed and in what format?</i>	[Describe the format in which data will be exchanged, e.g., CSV]
Date Range: <i>Tip: What date range will the data cover?</i>	[Describe any time-based filters to apply to the data, if applicable, e.g., data added in the previous quarter]

This agreement is compliant with [relevant controls]

Other Filters:	[Describe any additional filters to be applied to the data, e.g., children under 5]
-----------------------	---

Element – Short Name	Element – Long Name	Format
<i>Tip: Which data elements will be shared? For ideas on data needed to conduct the data match, send outreach, and evaluate the project, see "Selecting Data Fields" on page 39 of Data Sharing to Build Effective and Efficient Benefits Systems. You can also make this into a Technical Specification Document that is appended to the DSA.</i>		
EXAMPLE: BIRTH_DATE	Participant's Date of Birth	Char(8) MMDDYYYY

Section 2: [Primary Entity] will supply the following data to [Third Party Entity]:

Tip: The purpose of this section is to set up the data transfer from the Primary Entity to the Third Party Entity. This is predicated on the Primary Entity being the one to do the data match between program rolls and share data with a third party. Therefore, this section may need to be adjusted or removed depending on the arrangement for your initiative.

Frequency:	[Describe how often (and how many times) data will be exchanged, e.g., quarterly, four times]	
Method of Transfer:	[Describe how data will be exchanged between entities, e.g., SFTP]	
File Format:	[Describe the format in which data will be exchanged, e.g., CSV]	
Date Range:	[Describe any time-based filters to apply to the data, if applicable, e.g., data added in the previous quarter]	
Other Filters:	[Describe any additional filters to be applied to the data, e.g., children under 5]	
Element – Short Name	Element – Long Name	Format

This agreement is compliant with [relevant controls]

Section 3: [Primary Entity] will supply the following data to [Secondary Entity]:

Tip: The purpose of this section is to provide the Secondary Entity with data so that it can know which of its participants have been identified as likely eligible for additional benefits, as well as for any evaluation needs.

Frequency:	[Describe how often (and how many times) data will be exchanged, e.g., quarterly, four times]
Method of Transfer:	[Describe how data will be exchanged between entities, e.g., SFTP]
File Format:	[Describe the format in which data will be exchanged, e.g., CSV]
Date Range:	[Describe any time-based filters to apply to the data, if applicable, e.g., data added in the previous quarter]
Other Filters:	[Describe any additional filters to be applied to the data, e.g., children under 5]

Element – Short Name	Element – Long Name	Format

Section 4: [Third Party Entity] will supply the following data to [Primary Entity] and [Secondary Entity]:

Tip: The purpose of this section is to provide the Primary Entity, and as needed Secondary Entity, with data from the Third Party Entity regarding the outcomes of outreach efforts, independent evaluation analysis, etc. This is predicated on the involvement of a Third Party Entity that will need to share information back to the other entities. Therefore, this section may or may not be necessary for your initiative.

Frequency:	[Describe how often (and how many times) data will be exchanged, e.g., quarterly, four times]
Method of Transfer:	[Describe how data will be exchanged between entities, e.g., SFTP]
File Format:	[Describe the format in which data will be exchanged, e.g., CSV]
Date Range:	[Describe any time-based filters to apply to the data, if applicable, e.g., data added in the previous quarter]
Other Filters:	[Describe any additional filters to be applied to the data, e.g., children under 5]

This agreement is compliant with [relevant controls]

Element – Short Name	Element – Long Name	Format

Article IV: General Provisions

Nothing in this Agreement shall be construed as authority for any party to make commitments that will bind any other party beyond **Article I** contained herein.

All parties agree to:

- 1) Adhere to all security standards as for secure data storage and transmission as expressed in [relevant data security standard, e.g., SOC 2 – Type II certification].
- 2) Prohibit and prevent re-disclosure of any other party’s data to any entity not covered by this agreement.
- 3) Prohibit and prevent storage of any party’s data on mobile or portable data storage media without:
 - a) Documented business necessity approved in writing by the data stewards of all parties.
 - b) Documentation that all data storage media are physically and logically secured and acknowledged by an Information Security Officer from each party.
- 4) Provide immediate notification to all other parties if a breach, loss, theft, or other compromise of sensitive electronic or physical data is suspected within 24 hours of discovery. Notification contacts are as follows:
 - a) [Primary Entity], [Contact Name], [Contact Title], [Contact Phone Number], [Contact Email]
 - b) [Secondary Entity], [Contact Name], [Contact Title], [Contact Phone Number], [Contact Email]
 - c) [Third Party Entity], [Contact Name], [Contact Title], [Contact Phone Number], [Contact Email]

Article V: Termination

Any party may opt out of this Agreement without cause upon [Number (#)] days written notice to all other parties.

Any party may opt out of this Agreement immediately, via written notice, upon discovery of a data breach suffered by any other party.

Any party may suspend its involvement in this Agreement immediately upon discovery of a data breach suffered internally. Suspension of this Agreement shall not last more than [Number (#)] days and this Agreement must either be reinstated or terminated per the terms of this Agreement by the end of that period. Suspension and reinstatement/termination must include written notice to all other parties.

This Agreement shall remain in full effect until replaced by a subsequent Agreement, unless sooner terminated as provided herein.

This agreement is compliant with [relevant controls]

This Agreement shall automatically be terminated upon:

1. Fulfillment of all terms; or
2. When superseded; or
3. After a period of [Number (#)] years

This Agreement [may/may not] be re-negotiated or renewed upon termination, following an appropriate review of all terms and conditions.

Article VI: Integration, Modification, and Assignment

This document represents the entire Agreement between all parties. Any modification of these terms must be in writing and signed by all parties. This agreement shall be interpreted in accordance with the laws of the [State]. Signed copies of this agreement, and any modifications, shall be kept on file with [Primary Entity and/or Secondary Benefit Entity] Office of Information Management.

#The remainder of this page is intentionally left blank#

Signatures

The undersigned hereby acknowledge and accept the responsibilities, terms, and conditions laid out in this Data Sharing Agreement:

NAME | Date
[Primary Entity]
TITLE

NAME | Date
[Primary Entity]
TITLE

NAME | Date
[Secondary Entity]
TITLE

NAME | Date
[Secondary Entity]
TITLE

NAME | Date
[Third Party Entity]
TITLE

NAME | Date
[Third Party Entity]
TITLE

#End of Document#

Appendices:

- a. Project Documentation



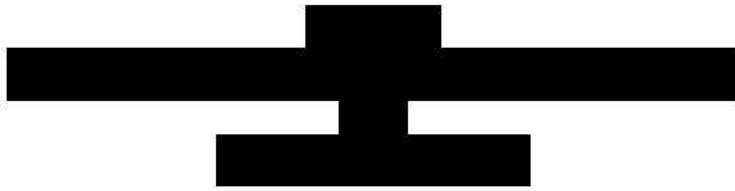
Appendix II: Sample Data Sharing Agreements

This appendix includes redacted and/or modified agreements from administering agencies that enable data sharing for outreach. They reflect specific use cases and are included for the purpose of illustrating data sharing concepts. All wording and formatting comes directly from the source. As a reminder, do not act or refrain from acting based on information in these agreements and the Playbook at large without first seeking legal advice from your legal counsel in the relevant jurisdiction.



[REDACTED]

Exhibit D – Data Sharing Agreement



This Data Sharing Agreement (Agreement) is entered into by and between [REDACTED] and [REDACTED] each individually a party and together the parties.

This Agreement shall take effect upon its signing by all parties. This Agreement may be amended at any time by written agreement of all parties. All parties will conduct an independent review of this Agreement on an annual basis. This Agreement shall remain in effect until September 30, 2023 (*date*), as determined by Contract or terminated by written notification from one party to another.

I. Financial Understanding

Note that the execution of this Agreement is contingent upon the availability of funds to implement the tasks outlined herein for any agreement where an exchange of funds occurs.

When applicable and not specified elsewhere, this Agreement serves as a non-financial understanding between Recipient and Provider. No financial obligation by or on behalf of either of the parties is implied by a party's signature at the end of this Agreement. The terms of any financial liability that arises from data processing activities carried out in support of the responsibilities covered herein must be negotiated separately and to the mutual satisfaction of the parties. The legal authority for data sharing for specified purposes conveyed by this Agreement cannot be used to support a subsequent claim of implied agreement to financial obligation.

II. Background

Provider is charged with providing resources for children, families, and early care professionals to best prepare [REDACTED] for future success, including the secure collection of data to assess program implementation and efficacy. Recipient is an organization responsible for the implementation of outreach efforts that aid in the administration or enforcement of the SNAP Program in accordance with 7 CFR 272.1(c)(1). Provider believes in collaborating with all partners to design and deliver high quality human and health services that improve the safety,

independence, and well-being of the people of [REDACTED] Provider and Recipient will work together on this objective. This Agreement applies to all data sharing between Provider and Recipient. Specific data to be shared are outlined in attached appendices, along with the purpose of data sharing, data ownership and conditions and/or regulations governing the usage of the shared data. Also in the appendix will be further requirements for shared data retention/destruction, and Recipient processes for implementing these actions.

III. Purpose

Provider and Recipient enter into this Agreement to share and exchange Data for the purpose of improving practice and policy development. Details of data to be shared are outlined in attached Appendices. The appendix will also define the federal and state governing authorities, e.g. HIPAA, 42 part 2, FERPA or others. If two or more governing authorities are defined, the most restrictive governance will apply. If this agreement is between state agencies, the Business Associate Agreement signed with this Agreement will apply to all data sharing between Provider and Recipient. For all other parties, the Business Associate agreement applies only to the specific transaction associated with this agreement.

IV. Use

- A. This Agreement shall be used exclusively for the purposes of sharing Data with the intentions of using the Data for decision making, publishing, reporting, longitudinal analysis, research, and policy making, permitted by the applicable governing authorities. Recipient shall demonstrate that the requested data will only be used for authorized purposes when/where applicable and as noted in appendices. All Data sharing under this Agreement will be shared following applicable regulations required by the Provider, i.e. FERPA, HIPAA, or other information security/privacy requirements.

VI. Data Accuracy

- A. The Data is current as of the date and time compiled and can change. Provider does not ensure 100% accuracy of all records and fields. Some data fields, including those that are not used, may contain incorrect or incomplete Data. Recipient will report any systematic problems with the Data identified in linked data sets to the Provider.

[REDACTED]

VII. Confidentiality

- A. The parties, including their contractors and subcontractors, agree to protect Data according to acceptable standards and no less rigorously than they protect their own confidential information. Protected information will not be reported or made public.
- B. Recipient shall not disclose, release, reveal, show, sell, rent, lease, loan or otherwise grant access to Protected Data and/or any Data derived or extracted, to any individual who does not need the Data to complete their work assignment as required by their job responsibilities within the scope of this Agreement. This includes reports, written or oral presentations, written analysis, study articles or any similar documents containing Data.

VIII. Data Governance Plan & Data Controls

- A. Both parties agree to have in place a Data Governance plan with support and participation from across their organizations that detail the parties' policies and procedures to protect privacy and data security, including ongoing management of training, data collection, processing, storage, maintenance, use and destruction. Provider has the right to conduct audits or other monitoring of the other Party's Data Governance policies, procedures, and systems. If, through these monitoring activities, vulnerability is found, the Recipient must take timely appropriate action to correct or mitigate any weaknesses discovered.

IX. Security Controls

- A. Any data sharing under this Agreement by parties will comply with the [REDACTED] Information Security and Privacy Policies and Governance Rules, and Standards [REDACTED] issued under the authority of [REDACTED] or other agreed upon information security controls attached as an addendum to this Agreement. Recipient shall comply with the most restrictive information security policy. Recipient shall include the terms of this Agreement and make them applicable to any third-party.
- B. Provider will hold Recipient accountable to ensure their Data is handled by the authorized individuals necessary to achieve the stated purposes, while still conforming to all regulations and security policies.

[REDACTED]

X. Access Restrictions & Minimization

- A. The specific records to be released from Provider shall be subject to the written consent of Provider's Data Governance Manager (or designated authority as noted in Appendix A).
- B. The Data recipient shall prohibit the use of non-organizational furnished equipment to access data shared pursuant to this agreement. *Note: personally owned devices can be used to access the data through an organizational provided virtual environment.)*
- C. Both parties attest that the data requested represent the minimum necessary information as described herein and represent the minimum necessary information individuals will have access to in order to perform the work.

XI. Re-disclosure of Data

- A. Without authorization from the Data Governance Manager (or designated authority) of the Data Provider, or where such disclosure is expressly prohibited, the Data Recipient may only further disclose data in an aggregate form that de-identifies or anonymizes the data.

XII. Data Retention

- A. Recipient agrees to safely maintain Data while conducting the research (or work scope) specified in the Agreement. All unnecessary records shall be purged within 6 months from the time it was released to the Recipient, or sooner if it has been determined if they no longer serve the stated purpose or provide potential research value. Records shall either be returned to the Provider or destroyed in a secure manner. Data retention policies shall comply with the [REDACTED]
- B. With a written permission Recipient may employ third-parties to provide a service or function on its behalf. Recipient ensures all terms are passed to any third-party.

XIII. Provider Duties

- A. The Provider shall maintain ownership of the Data.
- B. The Provider maintains ownership in the case of third-party vendors who may house agency Data off-site as a part of the longitudinal data linking process.
- C. The Provider shall ensure that all identifying information is transmitted through secured encrypted connections.
- D. The System Steward and Providers will agree on and carry out any additional security or steps that are required as a result of the Risk Assessment to ensure the integrity of the linked data, up to and including the decision not to release the linked data.

XIV. Recipient Duties

- A. The Recipient maintains a stewardship role for the preservation and quality of the Data.
- B. The Recipient shall not retain any right, title or interest in any of the Data furnished by the Data Provider.
- C. The Recipient may use and disclose Data as permitted in this Agreement and only in a manner that does not violate state, or federal privacy regulations.
- D. The Recipient shall implement appropriate safeguards to prevent use or disclosure of Data not authorized by this Agreement.
- E. The Recipient shall ensure that the Data are kept in a secured environment (commensurate with level of data sensitivity) at all times and that only Authorized Users have access.
- F. The Recipient shall report within 1 business day to the Provider any use or disclosure of the Data of which the Recipient becomes aware that is not provided for or permitted in this Agreement.
- G. The provider requires that each Authorized User complete a valid Confidentiality Agreement Form, See Appendix B, Sample Confidentiality Agreement Form before access to the data is granted. The Recipient shall maintain a file of executed forms, and produce them for review upon [REDACTED] request.
- H. The Recipient shall permit the Data Provider to investigate any such report and to examine the Data Recipient's premises, records and practices. The Recipient agrees to abide by the resulting notification procedures outlined by the Provider in the event of a breach.

XV. System Steward Duties

- A. System Stewards maintain a stewardship role for the preservation and quality of the Data.
- B. System Stewards shall manage their system, and ensure the integrity and safety of the Data at all times.
- C. System Stewards shall implement appropriate safeguards to prevent use or disclosure of Data not authorized by this Agreement and the attached appendices.
- D. System Stewards shall ensure that the Data are kept in a secured environment at all times while under their control and that only Authorized Users have access.

XVI. Linked Datasets

The result of linking different system data sets is a new data set that potentially has unique regulations and conditions governing its release and use.

- A. Prior to release of linked data, the System Steward will classify the linked data according to risk of data breach. This could include evaluating based on means of release, or on likelihood of identifying personally identifiable information from the linked data (or violating other regulations that apply to the linked data).
- B. Based on the above classification, if protected information will be released, a Risk Assessment shall be conducted prior to release by System Steward.
 - a. The following questions shall be asked by System Provider:
 - i. Does the linked data meet the original request and can it be used how the Recipient planned?
 - ii. What conditions and/or regulations apply to the linked data?
 - iii. Does usage of the linked data pose a high risk of breaching those regulations?
 - iv. Have reasonable and appropriate steps been taken to reduce the risk of breach during the actual transfer of data to the Data Recipient?
 - v. How will the data be protected at rest and in transit?
 - vi. Others as required.
 - b. Results of the Risk Assessment shall be provided to Provider for review.

- c. Based on the results of the Risk Assessment and recommendations from Provider, the System Steward shall apply additional constraints as necessary to the usage of the linked data. Provider shall require the following minimum constraints:
 - i. Require Recipient to destroy data after 6 months (or less if the risk is determined to be high), with accompanying proof of destruction submitted to System Steward,
 - ii. The System Steward must follow-up after specified time period to review results of data usage by Recipient; and
 - iii. Recipient must demonstrate that no protected data was released to unauthorized third-parties,
 - iv. Others as required.

Final agreement on additional constraints shall be documented in the Appendix, and signed by the Providers, the Requestors and System Steward as appropriate, prior to release of Linked Data.

XVII. Accountability: Unauthorized Access, Acquisition, Use, Disclosure

- A. Recipient shall make a good faith effort to identify any use or disclosure of Protected Data not authorized by this Agreement.
- B. If either Party becomes aware of any Incident involving shared Data, it shall notify the other Party immediately and shall cooperate regarding recovery, mitigation, remediation, and the necessity to involve law enforcement.
- C. In the event a Data Breach occurs as a result of data sharing, the Recipient shall be responsible for notifying Provider within 1 calendar day and working with the respective Data Governance Managers (or delegates as noted in Appendix A) in contacting and informing the individuals in accordance with the applicable breach laws who may have been affected by the security breach. Recipient may not contact such individuals prior to notification of Provider management.
- D. Should Recipient not comply with this Agreement, Recipient may be subject to sanctions, including but not limited to denial of access and end to the agreement.
- E. In the event of a breach or unauthorized release of data held by recipient, recipient shall be liable for all costs of remediation, mitigation, etc. as such actions may be required to meet the security requirements of Provider or otherwise required by law.

XVIII. Survival

The respective rights and obligations of parties shall survive the termination of this Agreement with respect to Data previously shared.

V. Default Definitions

42 part 2 means the federal law that protects substance abuse records held by part 2 program.

Authorized User means an individual who has been granted the appropriate privileges and rights to access an information technology system and view the data contained within (as defined in the respective department's data sharing policy).

Consolidated Agency refers to those state agencies whose IT functions were consolidated under [REDACTED] pursuant to [REDACTED] and defined in [REDACTED]

Data means the representation of facts including but not limited to texts, numbers, graphics, images, sounds, or video. Facts are captured, stored, and expressed as Data.

Data Breach means a security (or privacy) incident that meets specific legal definitions as per state and federal breach laws.

Data Participant means an individual who provides, receives, analyzes and reports results of shared data.

Data Governance means the oversight of data quality, data management, data policies, business process management, and risk management surrounding the handling of data, and includes a set of processes that ensures that important Data assets are formally managed throughout the State Agency, department organization, or enterprise.

Data Governance Manager means the individual responsible for the implementation and oversight of the State Agency's data management goals, standards, practices, processes, and policies. Each Agency's Data Governance Manager is authorized, after following approved internal Data Governance policies, to approve the sharing and release of that Agency's or Program's data to entities outside of that Agency or Program.

Data Providing Participant means the party having the responsibility and authority for an entrusted data resource. The Data Owner plays a key role in internal Data Governance within each State Agency or related Program. The Data Owner takes ownership of the operational, technical, and informational management of the Data. The Data Owner knows how to use the data, to whom it can be released and the appropriate conditions and regulations that govern the use of the data.

[REDACTED]

Data Steward means individuals who manage and/or house data elements and/or categories at various points in the data lifecycle.

Event: A change of state for the management of data or IT services. An event can also mean an alert indicating an unwanted or undesired change of state possibly affecting data or IT services.

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g, means the federal law that protects the privacy education records holding students' personally identifiable information.

Demographic Data Set means a set of demographics that uniquely define a particular person, often considered PII.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and regulations promulgated thereunder by the U.S. Department of Health and Corrections (the "HIPAA Regulations"), means the federal law that establishes privacy and security standards to protect patients' medical records and other health information held by covered entities.

K-12 means school education levels ranging from kindergarten to high school graduation.

Linked Data means the resultant data set after two or more agencies' data have been linked through the link system.

Longitudinal Analysis means an analysis of data or a population over time.

Non-Consolidated Agencies refers to those state agencies whose IT functions were not consolidated under [REDACTED].

Personal Identifying Information (PII) means Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

[REDACTED]

PII also means a dataset that is linked to a specific individual and that would allow a reasonable person, who does not have knowledge of the relevant circumstances, to identify the individual with reasonable certainty.

Any statutorily applicable definition will supersede this definition.

Privacy Incident: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, have access or potential access to PHI/PII in usable form, whether physical or electronic, or where authorized users access PHI/PII for an unauthorized purpose.

Protected Health Information (PHI) means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to 45 C.F.R Section 164.501.

Protected Information means PII, PHI, Federal Tax Information, and Social Security Information, sensitive or other data protected under local, state or federal law or by policy.

Risk Assessment of Linked Data is a review conducted of the results of two or more pieces of data linked together by systems to answer a specific research or educational question. The focus of the Risk Assessment is to determine the level of risk (related to a data breach) introduced by combining data. The individual data Participants will contribute to the Risk Assessment to help determine if the new data set may have unique regulations and conditions governing its release and use not present prior to combining the data.

Role-Based Access means a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.

Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Single Source Of Truth (SSOT) as used in Information Systems design and theory, SSOT means the practice of structuring information models and associated schemata such that every data element is stored exactly once (e.g. in no more than a single row of a single table). Any possible linkages to this data element (possibly in other areas of the relational schema or even in distant federated databases) are by reference only. Thus, when any such data element is updated, this update propagates to the enterprise at large, without the possibility of a duplicate value somewhere

[REDACTED]

in the distant enterprise not being updated (because there would be no duplicate values that *needed* updating).

State Agency means each principal department within the executive branch, including each board, division, unit, office, or other subdivision within each department, each office or agency within the Governor's Office, each state-supported institution of higher education, and each local district junior college; except that State agency shall not include any department, agency, board, division, unit, office, or other subdivision of a department that does not collect unit records.

System Steward means the agency responsible for running and managing the "Link" data system. The relevant agency will ensure that the provided data will be handled with care, following all applicable [REDACTED] information security policies. When the Linked Data is produced from combined agencies systems, all involved Data Owners will participate in validation and risk assessments as defined in this Agreement.

APPENDIX A – SAMPLE BUSINESS USE CASE

I. Purpose

- A. [Insert a detailed summary of the purpose for requesting the data, information about the purpose for requesting the data and any other background applicable to the analysis or study being conducted.]

II. Roles

- A. The System Steward for this use case is First Name, Last Name, Title, email address, business phone number. *If applicable.*
- B. The Recipient is [Insert First Name, Last Name, Title, email address, business phone number].
- C. The Provider is [Insert First Name, Last Name, Title, email address, business phone number].
- A. The Data Governance Manager for Participant is [REDACTED]
- D. Data Governance Manager for Recipient is [Insert First Name, Last Name, Title, email address, business phone number].
- E. Recipient staff with permission to view, access, or use Data include:
- [Insert First Name, Last Name, Title, email address, business phone number].
 - [Insert First Name, Last Name, Title, email address, business phone number].
 - [Insert First Name, Last Name, Title, email address, business phone number].
- F. Recipient may identify additional staff who require access to Data and provide that request to Provider in writing for review and consideration.

III. Request

- A. [Insert a summary of what data is being collected, the reason why personally identifiable information is required, and the purpose for collection.]
- B. [Insert a summary how the data will be transmitted]
- C. [Insert a summary a schedule of the data transfer]

IV. Output

- A. [Insert a summary of the output. This section states what reports or information will be produced because of this data transmission and where that information will go.]

V. Data Linkage

A. [Insert detailed information on the Data being linked, the other sources of Data, and any additional constraints to protect the linked Data.]

VI. Participating Parties

A. The Provider will be sharing data with the [Insert Organization Name].

VII. Duration of Study

A. The study referenced in this Appendix will end on [Insert the date the sharing ends.]

VIII. Processes

A. [Insert information on how the data will be used, what kinds of analysis will be done with the data, and other purposes for using the data.]

IX. Table of Required Data and Ownership

N o.	Table Name	Column Name	Column Description	Data/Product Owner
1				
2				
3				

X. Regulations that Apply

- 1. FERPA (34 CFR Part 99, section 99.3)
- 2. HIPAA Section 164.514(a)-(c) (CFR. Title 45, Parts 160, 162, and 164)
- 3. The Student Data Transparency and Security Act (C.R.S. 22-16-101 et. all.)

Additional:

[REDACTED]

Constraints,

Definitions,

Confidentiality Requirements,

Program Specific Items,

Signatures

To further the collection and analysis of [REDACTED] to benefit the public, Recipient represented by the *(TITLE), (NAME)*, and Provider, represented by *(TITLE), (NAME)* of [REDACTED], agree to the cooperative sharing of data between the two parties pursuant to the conditions set forth herein.

Signature: _____

Date: ___/___/___

(NAME)

(TITLE)

(Recipient Organization)

Signature: _____

Date: ___/___/___

(NAME)

(TITLE)

[REDACTED]

**APPENDIX B,
SAMPLE - Food and Energy Confidentiality Agreement**

I, _____, understand that in the course of my employment or contract with the _____ its offices, agencies and/or departments either by direct contract or through agreements between State offices, agencies or departments I may receive or become aware of business or personnel information that is sensitive and/or confidential and not available to the general public.

This information may be written, electronic, or verbal and come from a variety of sources. I understand that this information may be subject to special protections under State or Federal laws or policies of the State office, agency or department. I understand that I am not to intentionally access sensitive or confidential information unless it is necessary in order for me to complete my job responsibilities and if so, such necessity will be set out in a statement of work regarding the specific project I am working on.

I acknowledge that I have an affirmative responsibility to protect all sensitive or confidential information I become aware of during the course of my duties. I further understand that this obligation does not apply to information I may become aware of that is available to the general public, through common knowledge or internet search.

I understand that in the performance of my duties I may be requested to provide sensitive or confidential information to others. I agree to hold in confidence and to not disclose any sensitive or confidential information to any person, including employees of state, federal or local governments including law enforcement, except to those who have an official business reason for the information. Should I have any questions regarding the proper handling or disclosure of confidential or sensitive information, I will immediately notify my supervisor or manager and/or the supervisor or manager of the project I am working on for further clarification and direction prior to releasing any information.

If I willfully and knowingly disclose such information in any manner to any person or agency not entitled to receive the information, I understand that I may be subject to adverse action, including corrective or disciplinary action, dismissal or personal liability depending on the severity of my actions and applicable law. It is my duty and responsibility to return all State information and not to retain any copies, in any format upon the completion of my employment or contract.

I acknowledge that I have read, understand and will adhere to the above requirements with respect to sensitive and/or confidential information.

Signature: _____

Printed name: _____

Date: _____

Data Recipient should maintain a copy of the executed form and provide it upon request

[Redacted] Data Sharing Agreement

WHEREAS, the Parties have collaborated to implement a data-driven strategy that will enhance SNAP enrollment for seniors (the Initiative) as described in the Parties' Grant Award;

WHEREAS, --- maintains individually identifiable demographic information on applicants and recipients applying for and participating in "SNAP" ;

WHEREAS, --- administers the Supplemental Nutrition Assistance Program ("SNAP") for the State of --- and is responsible for accepting and processing applications for low-income clients;

WHEREAS, --- seeks to use the Medicaid data specified herein for the purpose of identifying low-income individuals eligible for, but not receiving SNAP assistance, in order to conduct outreach to such individuals, assist them in applying for SNAP;

[Additional sections redacted]

NOW, THEREFORE, the Parties to the DSA agree to the following terms and conditions:

Article I: Terms of Agreement

This DSA shall commence on the Effective Date set forth above and shall expire on... In the event that a new Memorandum of Understanding or standalone DSA is not signed on or before the expiration of this agreement, the terms of this DSA shall remain in full effect until replaced by a subsequent DSA, unless terminated sooner as provided herein.

Article II: Data Sharing Specifications

1. Data Recipient shall:
 - a. Adhere to the terms and conditions provided for in this Agreement
 - b. Restrict access to the data disclosed under this Agreement to only those individuals authorized to perform the services described herein, ("Data Users") and shall ensure that the Data Users are under the direction and control of Data Recipient at the time of the Data Users' performance of any such services utilizing secure access protocols. Data Users include employees or individuals providing services stated herein.
 - c. Require that each Data User complete a valid Confidentiality Certification Form before access to the data is granted. Data Recipient shall provide --- a copy of each completed Confidentiality Certification Form, maintain a file of executed forms, and produce them for review upon --- request.
 - d. Monitor the use of and access to the data by the Data Users to ensure the data is secured and used in a manner and purpose consistent with this DSA.
 - e. Retain all data disclosed under this DSA secured in a manner that ensures it is kept confidential; develop and require all Data Users to follow security procedures designed to keep the data confidential; limit its access to only authorized Data Users; and ensure that all transfers of data are made in a secure manner.
2. --- will work with --- to conduct a data match of Medicaid households with at least one senior, 60 or older, against the file of SNAP enrolled households. The resulting file(s), containing current

Medicaid, 60 or older who are not enrolled in SNAP, will be provided to the Data Recipient. The SNAP data file provided by --- shall include the following data fields:

Column Name	Description	Format
FIRST_NAME	The individual's first name	Text
LAST_NAME	The individual's last name	Text
ADDRESS_1	The individual's mailing address line 1	Text
ADDRESS_2	The individual's mailing address line 2	Text
CITY	The individual's mailing city	Text
ZIPCODE	The individual's mailing zip code	5-digit number
PHONE_NUMBER	The individual's phone number	10-digit number
BIRTH_DATE	The individual's date of birth	ISO 8601 formatted date (YYYY-MM-DD)

Table 1 - Outreach File Column Descriptions

3. --- shall provide all electronic files via an encrypted file through a File Transfer Protocol (FTP) secure account upon commencement of this Initiative and on at least a monthly basis moving forward or as otherwise specified in the Parties' Memorandum of Understanding). The data shall remain in the encrypted file during the transfer and while it is received and held by --- .

[Additional sections redacted]

Article III: Legal Basis for Disclosure of Confidential Client Information

1. Medicaid data is confidential and protected by federal law pursuant to 42 United States Code 1320d et. seq., federal regulations promulgated under 42 C.F.R. Part 431.302 and the Health Insurance Portability and Accountability Act (HIPAA"), 45 C.F.R. Parts 160, 162 and 164 et. Seq.

[Additional sections redacted]

2. Data Recipient intends to use the data specified herein for the purposes of identifying low-income seniors eligible for, but not receiving SNAP benefits, for the purpose of conducting outreach to such individuals to assist them in applying for SNAP and where possible confirming the enrollment of individuals whom Data Recipient assists in completing a SNAP benefits application.
3. --- acknowledges that increased enrollment of low-income seniors for SNAP benefit is directly connected with medical assistance programs in that better nutrition leads to positive health outcomes and reduced health care costs.
4. Individually identifiable protected health information maintained by --- may be disclosed to the Data Recipient, absent individual consent, in accordance with Section 1396a of the Social Security Act which provides that State Medicaid plans must restrict the use and disclosure of medical assistance data concerning applicants and recipients to purposes that are directly connected with administration of the plan. 42 U.S.C. § 1396a (7)(A). The data disclosure contemplated in this DSA satisfies the definition of "directly connected" to the administration of medical assistance in that establishing eligibility and providing services for recipients are both valid purposes that are directly connected with the administration of medical assistance and therefore allow for the disclosure of Medicaid data absent individual consent. 42 C.F.R. §§ 431.300(a),431302. Moreover, the federal regulations provide that the confidential information exchanged should be made available only to the extent necessary to assist in the valid administrative needs of the program receiving the information. 42 C.F.R. § 431(b)(l).

5. Medicaid records contain HIPAA protected health information and may be disclosed absent individual consent in accordance with the Treatment, Payment Health Care Operations (TPO) exception to the HIPAA consent requirement. 45 C.F.R. §164.506 (c)(1), which provides that a covered entity may use or disclose protected health information for its own health care operations without individual authorization. 45 C.F.R. §164.506 (c)(1). HIPAA defines health care operations as population-based activities that relate to the Improvement of health or reduction of health care costs, protocol development, case management and care coordination and related functions that do not include treatment. 45 C.F.R. §164.501.
6. Addressing the state entity's legal ability to share individual level SNAP data, federal regulations restrict use and disclosure of information obtained from Supplemental Nutrition Assistance Program (SNAP) applicants or recipients to certain persons, including persons directly connected with the administration or enforcement of the provisions of the Food and Nutrition Act or regulations, other Federal assistance programs, federally-assisted State programs providing assistance on a means-tested basis to low income individuals, or general assistance programs which are subject to the joint processing requirements. 7 C.F.R. 272.1(c)(1). Data Recipient, through its relationship with ---, is directly connected to the administration and enforcement of SNAP and shall use and share any information obtained from SNAP applicants and recipients solely for that purpose. Additionally, as an authorized recipient of SNAP information, Data Recipient shall adequately protect the information against disclosure for any unauthorized purposes as required by federal regulations. 7 C.F.R. 272.1(c)(2).

Article IV: Confidentiality

1. Security and Confidentiality of Personally identifying and other Confidential Client Information. Data Recipient agrees to be fully responsible to --- for the security of the storage, processing, compilation, and transmission of all personally identifying and other confidential client data supplied to It by ---, and of all equipment, storage facilities, transmission facilities on or from which any such data is stored, processed, compiled, or transmitted.
2. Data Recipient agrees that it will not access, use, or disclose such data supplied by --- beyond its limited authorization under this DSA or for any purpose outside the scope of this DSA.
3. Data Recipient agrees that it will protect such data in a secure environment and ensure that its computer site(s) and related infrastructure will have adequate physical security and that in situations such as remote terminals or other office work sites where all the requirements of a secure area with restricted access cannot be maintained, the equipment shall receive the highest level of protection and shall be consistent with Internal Revenue Service publication requirements on alternate work sites. Data Recipient agrees that it will not allow any such data supplied to it by --- to be held on mobile, remote, or portable storage devices.
4. Data Recipient agrees that it will protect the confidentiality of such data in accordance with the requirements of all applicable state and federal laws, regulations, standards, and guidelines, as well as all applicable industry standards, including, but not limited to, Internal Revenue Service requirements, federal Information processing standards, the federal Privacy Act, Payment Card Industry ("PCI") data security standards, and functional and assurance requirements for the operating security features of Its systems.
5. Data Recipient agrees that it will ensure that appropriate background checks are performed on each employee/agent/subcontractor to whom It grants access to any such data; that it will ensure that an appropriate and effective authorization process for user access is maintained; that it will ensure that each of its employees and agents to whom data is disclosed is notified in writing of the

confidentiality and security requirements of this DSA and of criminal and civil sanctions under applicable laws; and that It will notify --- immediately in writing if the relationship ends between Data Recipient and any employee/agent/subcontractor to whom it granted access or who obtained access to any --- data.

6. Data Recipient agrees that, in the event of any unauthorized disclosure or loss of such data supplied to it by ---, it will immediately notify --- of the extent of the breach of security, the reason therefore, the sources, the affected data, and mitigation actions. The Parties agree that the actual harm to a third party caused by a security breach is difficult to estimate, and that a reasonable forecast of just compensation is for the Data Recipient to provide to such individual: (1) timely and adequate notice of the facts surrounding the compromise of information; (2) actual damages sustained by the individual as a result of the breach and any prescribed or ordered damages; and (3) two (2) years of credit monitoring services, at no cost to such individual.
7. Data Recipient may not re-disclose the data to any persons or entities other than its Data Users. Data Recipient may not sell, share, or provide the data shared under this DSA with any third-parties.
8. Data Recipients may not publish the data in any form or re-format the data, except as follows: in aggregate form, with no data identifiable to any one individual, as part of the written outcome evaluation report. Any published --- data should be sufficiently de-identified to eliminate the risk of re-identification.
9. Data Recipient may not use the data for any purposes other than those described in this DSA.
10. Data Recipient agrees to hold all information, records or data obtained in the course of this data exchange confidential and such data shall not be disclosed to any person, organization, agency or other entity except as provided for herein. Data Recipient further agrees to abide by the provisions of any and all applicable federal, state and local laws and their implementing regulations, including but not limited to the Federal Social Security Act, the Federal Food and Nutrition Act, and any regulations promulgated thereunder, and all other confidentiality laws, regulations and requirements as may now be, or in the future may become, applicable. These authorities include but are not limited to: Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, and the Health Insurance Portability and Accountability Act, 45 CFR Sections 160, 162 and 164, 42 U.S.C.S. Part 2.
11. No individually identifiable Information obtained In the course of this data exchange shall be released to any other individual, non-participating agency, organization or entity without the prior consent of ---. Data Recipient shall permit --- to monitor its use of the data, including but not limited to promptly granting --- access to Its books and records upon request.
12. Notwithstanding any other agreement among or between the parties, --- and the Data Recipient agree to use appropriate safeguards to prevent the use or disclosure of any confidential and/or individually identifiable protected health information, and to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, Integrity, and availability of any electronic individually identifiable health information that it creates, receives, maintains, or transmits pursuant to this DSA. Access or use of confidential and/or identifiable protected health information shall be restricted to Data Users required to use such data In performance of their duties pursuant to this DSA and upon the signing of a confidentiality statement agreeing to keep such data confidential and agreeing to adhere to the confidentiality terms and conditions stated herein.
13. If Data Recipient's officials, employees, or Data Users fall to abide by any requirements of this DSA, Data Recipient must institute disciplinary action against such individual(s) up to and including termination. This provision in no way limits the remedies available to --- in the event that the Data

Recipients, its officials, employees, or Data Users fail to abide by the requirements of this DSA, including terminating this DSA and/or Data Recipient's access to --- data.

[Article V redacted]

Article VI: Effect of Unauthorized Disclosure

1. Notwithstanding any other agreement among or between the parties, Data Recipient agrees to immediately report in writing to --- upon discovery of any unauthorized use or disclosure of confidential or protected --- data, including individually identifiable health Information of which It becomes aware. Further, Data Recipient agrees to report to --- in writing upon discovery of any data security incident of which it becomes aware, including a breach of unsecured protected data.
2. Notwithstanding any other agreement among or between the Parties, in the event of an unauthorized disclosure of protected data or if Data Recipient knows or has reason to believe that confidential data may have been disclosed to entities or persons without proper authorization, including such disclosure by a Data User, the Data Recipient shall:
 - a. Immediately commence an investigation to determine the scope of the unauthorized disclosure to determine if a data breach occurred and shall draft an incident report containing such findings, Including the identity and number of the individual{s} whose protected data was, or is reasonably believed to have been the subject of the breach.
 - b. Promptly notify --- in writing of the breach when it is discovered, but no later than ten (10) business days after discovery.
 - c. At the discretion of --- or as required by law or regulation, promptly notify the affected individual(s) about a breach of the confidential data and/or individually identifiable protected health information, as soon as possible but not later than thirty (30) calendar days after discovery of the breach, except where a law enforcement official determines that a notification would Impede a criminal investigation or cause damage to national security. Notification shall be in a form and format prescribed by --- and shall meet the requirements of applicable local, state and federal law. Data Recipient shall bear all costs related to breach notification that involved the authorized disclosure of any --- data within the Data Recipient's possession. In the event of a breach of HIPAA protected health information, --- will be responsible for notifying the Secretary of Health and Human Services of the data breach, as required by regulation.

Article VII: Modification

1. Any modification or amendment of this Agreement shall be in writing and signed by Data Recipient and --- . Notwithstanding any modifications or amendments, the remainder of the Agreement shall remain in force.

Article VIII: Termination

1. The DSA may be terminated by either the Data Recipient or --- upon thirty (30) days' advance written notice to the other Party.
2. Data Recipient agrees to cease its use of --- data from the date of the termination of this DSA, unless otherwise instructed by --.

**Michigan Department of Health and Human Services
Intra-Agency Agreement Between the Women, Infant, and Children (WIC)
Program and The Michigan Department of Health and Human Services to
Share Confidential WIC Information
Under 7 CFR 246.26(d)(2) and (h).**

1. Purpose

This agreement between WIC and the Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) allows WIC to share applicant and participant information, including past participant information, with MDHHS for the purposes provided for in 7 CFR 246.26. The parties understand that all WIC information about an applicant or client is confidential and may only be shared as otherwise provided for in this agreement. 7 CFR 246.26(d)(1)(i).

2. Definitions

Agreement: means this external agency agreement.

WIC Record(s): means any past, present, or future, applicant or participant information regardless of the media or source, provided by WIC to external agency.

Department: means the Michigan Department of Health and Human Services.

Incident: A threat or event that compromises, damages, or causes a loss of confidential or protected information (e.g., unauthorized disclosure of information, failure to protect user ID's, theft of computer equipment or WIC records, etc.)

WIC: Michigan Department of Health and Human Service, Women, Infant, and Children's Division.

3. Scope of Agreement:

7 CFR 246.26(h)(3)(i)(A) allows for WIC data to be used for the non-WIC purpose of establishing eligibility of WIC applicants or participants for the programs that will assist in cross enrollment efforts. Applicants and recipients of MDHHS-ESA programs may be eligible for WIC. Outreach will be conducted to inform the applicants about the possibility of WIC eligibility.

7 CFR 246.26(h)(3)(i)(C) allows for WIC data to be used for the non-WIC purpose of enhancing the health, education, or well-being of WIC applicants or participants who are currently enrolled in such programs, including the reporting of known or suspected child

abuse or neglect that is otherwise required by state law, that MDHHS-ESA Program administers.

7 CFR 246.26(h)(3)(i)(D) allows for WIC data to be used for the non-WIC purpose of streamlining administrative procedures in order to minimize burdens on staff, applicants, or participants in either the receiving program or the WIC Program.

The chief State health officer for Michigan has designated in writing the permitted non-WIC uses of the WIC information and has identified Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) as an appropriate recipient of WIC data for non-WIC purposes.

4. Security

Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) agrees to use appropriate safeguards to prevent use or disclosure of the information other than as provided by this agreement; (MDHHS WIC Sponsor may require description of the security procedures that will be in place and followed.):

A. The data will be shared electronically.

B. WIC will transfer the data in an encrypted file to Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) agrees to limit access to this information only to those described and authorized in this agreement.

C. The data will be saved to a shared drive that has limited access.

D. The data will be cross referenced with Michigan Department of Health and Human Service – ESA (FAP, MA, TANF) data. Michigan Department of Health and Human Service – ESA (FAP, MA, TANF) will then be able to develop a list of potential WIC recipients to contact.

E. A selected number of ESA Policy and Technology Staff will have access to the data.

5. Incident Reporting

If, after obtaining confidential WIC records, Michigan Department of Health and Human Service – ESA (FAP, MA, TANF) eligibility determines there has been a potential breach of confidentiality that may include WIC records, Michigan Department of Health and Human Service – ESA (FAP, MA, TANF) eligibility shall contact their respective

MDHHS WIC Sponsor named in this agreement of the breach within 24 hours of knowledge of the breach. The MDHHS WIC Sponsor shall complete the DCH-1422 Incident Report Form and submit the DCH-1422 to the MDHHS-Compliance Office at [REDACTED]@michigan.gov. To the extent allowed by law, Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility and the MDHHS WIC Sponsor shall cooperate with the MDHHS-Compliance Office in any investigation regarding a data incident involving WIC records.

6. Restrictions and Conditions of Use

Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) will sign an affidavit provided by the MDHHS-Compliance Office attesting that the information will be destroyed after it is no longer need or will be retained for a specified period of time.

7. Retention and Disposition of WIC Information

The data will be held for the duration of the project with is three years at which point it will be destroyed. Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) will sign an affidavit provided by the MDHHS-Compliance Office attesting that the information will be destroyed after it is no longer need or will be retained for a specified period of time.

8. Effective Date

The information sharing required by this agreement shall not be effective until applicants and participants have been notified as required by 7 CFR 246.26(h)(2). This may be accomplished by the WIC program updating a publicly available list of such programs, in conjunction with a client agreement notifying clients of such a list. This agreement shall remain in full force and effect until superseded or terminated. The effective dates will be July 1, 2020 – January 2023.

9. Termination

This agreement may be terminated at any time by mutual consent of the parties. This agreement may be terminated by either party on delivery of 30 days written notice to the other party. WIC reserves the right to immediately terminate the information sharing provided for in this Agreement for failure to comply with the requirements of this Agreement. This Agreement may be modified by either party as needed to comply with federal or state laws, rules, or regulations, or if changes in policies require modification. The parties will meet as needed to effect any necessary changes.

10. Agreement Contacts

WIC:

[REDACTED], Director

Phone Number: [REDACTED]

Email: [REDACTED]@michigan.gov

Michigan Department of Health and Human Service – ESA:

[REDACTED]

Phone Number: [REDACTED]

Email: [REDACTED]@michigan.gov

WIC and Michigan Department of Health and Human Service – ESA (FAP, MA, TANF eligibility) agree, by the signatures below of their authorized representatives, that they have read this agreement, understand it, and agree to be bound by its terms and conditions.

WIC:

[REDACTED], WIC Division Director

Date

[NAME OF ENTITY RECEIVING DATA]:

[REDACTED], Senior Chief Deputy Directory MDHHS

Date

COMPLIANCE OFFICE:

[REDACTED], Chief Compliance Officer

Date

APPENDIX B

Text-based Recertification Intervention

I. Purpose

█ administers the Supplemental Nutrition Assistance Program (“SNAP”) programs for the State of █ and is responsible for accepting and processing applications for low-income clients.

█ seeks to use █ data specified herein for the purpose of identifying individuals who are eligible for recertification of their SNAP benefits and conduct text-based outreach to such individuals by providing steps for timely recertification of SNAP, pathways for completing SNAP recertification, and resources for individuals who need help. █ will be providing this outreach in partnership with █ counties.

This Agreement represents a unilateral data sharing agreement wherein █ is acting as the Data Recipient and █ is acting as the Data Provider.

II. Authority

Federal regulations restrict use and disclosure of information obtained from SNAP applicants or recipients to certain persons, including persons directly connected with the administration or enforcement of the provisions of the Food and Nutrition Act or regulations, other Federal assistance programs, federally-assisted State programs providing assistance on a means-tested basis to low-income individuals, or general assistance programs which are subject to the joint processing requirements. 7 C.F.R. 272.1(c)(1)(i).

Data Recipient, through its relationship with █ is directly connected to the administration and enforcement of SNAP and shall use and share any information obtained from SNAP applicants and recipients solely for that purpose. Additionally, as an authorized recipient of SNAP information, Data Recipient shall adequately protect the information against disclosure for any unauthorized purposes as required by federal regulations. 7 C.F.R. 272.1(c)(2); and SNAP State outreach plan required under █ and SNAP State Outreach Plan criteria developed by FNS.

III. Contacts

A. The Primary Contact for the Provider is █

B. The Primary Contact for Recipient is [REDACTED]

C. The System Steward for the Provider is [REDACTED]

D. The System Steward for the Recipient is [REDACTED]

IV. Data Description

A. On a monthly basis, [REDACTED] shall provide Data Recipient with a data file containing SNAP participants who are due for recertification in the current month or the following month and have a recertification packet indicated as “generated” in [REDACTED]. Contents of the file will be limited to the agreed upon counties. The data file shall include the following data fields:

Variable	[REDACTED] column name	Variable type	Column width
First name	"FIRST_NAME"	VARCHAR2	(35 BYTE)
Last name	"LAST_NAME"	VARCHAR2	(35 BYTE)
Street address	"ADDRESS_1"	VARCHAR2	(100 BYTE)
City	"CITY"	VARCHAR2	(30 BYTE)
Zip code + 4	"ZIPCODE"	VARCHAR2	(10 BYTE)
State	"STATE"	CHAR	(2 BYTE)
Day Phone Number	"PHONE_NUMBER"	VARCHAR2	(50 BYTE)
Home Phone Number	"HOME_NUMBER"	VARCHAR2	(50 BYTE)
Message Phone Number	"MESSAGE_NUMBER"	VARCHAR2	(50 BYTE)
Date of birth	"BIRTH_DATE"	DATE	'YYYY-MM-DD'
Last four of social security number	"SSN4"	VARCHAR2	(4 BYTE)
Case ID	"EXTERNAL_HOUSEHOLD_ID"	CHAR	(7 BYTE)
Recertification due date	"RECERTIFICATION_DUE_DATE"	DATE	'YYYY-MM-DD'
Primary language	"PRIMARY_LANGUAGE"	CHAR	(2 BYTE)
County	"COUNTY"	VARCHAR2	(25 BYTE)
File produced	"FILE_PRODUCED_DATE"	DATE	'YYYY-MM-DD'

- B. [REDACTED] shall provide electronic files via an encrypted file through a Secure File Transfer Protocol (SFTP) account monthly. The data shall remain in the encrypted file during the transfer and while it is received and held by [REDACTED]
- C. [REDACTED] is the source of the data provided by the Data Provider. The county is responsible for providing aggregate outcomes data for evaluation purposes, per the established and executed MOU between [REDACTED] and the county.
- D. All unnecessary records shall be purged within 12 months from the time it was released, or sooner if it has been determined they no longer serve the stated purpose.

V. Applicable Regulations

The following protection regulations are applicable to the data being transferred:

- A. 7 CFR 272.1 (C)(1)(i); 7 CFR 272.1 (C)(2)
- B. [REDACTED]

VI. Authorized Users

- A. [REDACTED], Outreach Analytics Manager
[REDACTED], Analytics Manager
- B. All Authorized Users are required to sign Individual Confidentiality Agreements (Appendix C of the SNAP External Partner Data Sharing Agreement). Data Recipient must maintain copies of signed agreements and furnish them to Data Provider upon request.
- C. Data Recipient may identify additional staff who require access to Data and provide that request to Data Provider in writing for review and consideration.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Appendix III: Additional Resources

This appendix includes reports, examples, guides, and other materials produced by administering agencies and subject matter experts about topics explored throughout the Playbook. This list of resources is not exhaustive but is offered for further reading.



Consent

- Amy Hawn Nelson, Deja Kemp, Della Jenkins, Jessie Rios Benitez, Emily Berkowitz, TC Burnett, Kristen Smith, Sharon Zanti, Dennis Culhane, “Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration,” Actionable Intelligence for Social Policy, University of Pennsylvania, June 2022, [Weblink](#).
- Daniel Stein, et al., “Modernizing Consent to Advance Health and Equity,” Stewards of Change Institute, November 2021, [Weblink](#).
- Ginger Zielinskie, Lindsey B. Gottschalk, “Rising Equitable Community Data Ecosystems (ReCODE). The Voices We Trust: Building Equity Centered-Community Data Ecosystems That Work for Everyone,” March 2022, Data.org, [Weblink](#).
- World Economic Forum, “Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction,” July 2020, [Weblink](#).

Data Catalog/ Data Dictionary

- Centers for Medicare & Medicaid Services (CMS), “CDR Data Catalog,” Accessed November 29, 2022, [Weblink](#).
- National Library of Medicine, “Data Catalog,” Accessed November 29, 2022, [Weblink](#).
- U.S. Geological Services, “Data Dictionaries,” Accessed November 29, 2022, [Weblink](#).

Data Governance

- Amy Hawn Nelson, Jessica D. Tenenbaum, “North Carolina Department of Health and Human Services Data Sharing Guidebook,” Actionable Insights for Social Policy, University of Pennsylvania and NCDHHS Data Office, May 2022, [Weblink](#).
- Baltimore City, “Data Governance,” 2021, [Weblink](#).
- Beek Center for Social Impact + Innovation at Georgetown University and National Governor’s Association, “Data Labs Playbook: Establish Data Governance,” May 2022, [Weblink](#).
- California Health & Human Services, “Data Exchange Framework,” 2022, [Weblink](#).
- Colorado Governor’s Office of Information Technology, “Government Data Advisory Board,” 2022, [Weblink](#).
- Natalie Evans Harris, “Sharing Data for Social Impact: Guidebook to Establishing Responsible Governance Practices,” Beek Center for Social Impact + Innovation at Georgetown University, January 2020, [Weblink](#).
- Organisation for Economic Cooperation and Development (OECD), “Data Governance in the Public Sector,” 2019, [Weblink](#).

Data Sharing & Equity

- Actionable Intelligence for Social Policy, University of Pennsylvania, “A Toolkit for Centering Racial Equity Throughout Data Integration,” May 2020, [Weblink](#).
- Liz Buck, Alissa Beers, Waldo Mikels-Carrasco, “A Community-Centered Approach to Data Sharing and Policy Change: Lessons for Advancing Health Equity,” Center for Health Care Strategies and Data Across Sectors for Health, August 2022, [Weblink](#).
- The White House, “Advancing Equity and Racial Justice through the Federal Government,” January 2021, [Weblink](#).



Outreach Best Practices

- Ariel Kennan, Elle Meyers, “Best Practices for Accessible Content,” Beeck Center for Social Impact + Innovation at Georgetown University, September 2022, [Weblink](#).
- Center on Budget & Policy Priorities and Benefits Data Trust, “Toolkit: Increasing WIC Coverage Through Cross-Program Data Matching and Targeted Outreach,” March 2022, [Weblink](#).
- Code for America, “Encouraging Uptake of Benefits with Psychological Ownership Messaging: Quantitative Research Report,” August 2021, [Weblink](#).
- Digital Benefits Hub by the Beeck Center for Social Impact + Innovation at Georgetown University and American Public Human Services Association (APHSA), “Outreach + Awareness: Maximizing Impact Through Clear Communication,” 2022, [Weblink](#).
- Jessica Lasky-Fink, Jessica Li, Anna Doherty, Karla Palos, Charles Davis, Elise Dizon-Ross, Johanna Lacoë, Jesse Rothstein, “Outreach to California College Students Encouraged Them to Apply for CalFresh,” California Policy Lab, August 2022, [Weblink](#).

Other Resources

- Amy Hawn Nelson, Della Jenkins, et al., “Introduction to Data Sharing & Integration,” Actionable Intelligence for Social Policy, University of Pennsylvania, May 2020, [Weblink](#).
- California Health Care Foundation, “Data Exchange Explainer Series,” May 2022, [Weblink](#).
- Centers for Medicare & Medicaid Services (CMS), “Cross-Sector Data Sharing to Address Health-Related Social Needs: Lessons Learned from the Accountable Health Communities Model,” October 2022, [Weblink](#).
- Denise Chrysler, “Checklist of Information Needed to Address Proposed Data Collection, Access and Sharing,” The Network for Public Health Law, October 2019, [Weblink](#).
- Katie Sullivan, Sara Soka, Keith Barnes, “Text to Connect: Using Text Message Outreach to Reduce SNAP Churn,” Benefits Data Trust and Beeck Center for Social Impact + Innovation, October 2021, [Weblink](#).
- Khaliyl Lane, “Maximizing Linkages: A Policymaker’s Guide to Data-Sharing,” One Degree (formerly Alluma), April 10, 2019, [Weblink](#).
- Medicaid Innovation Accelerator Program, “Using Data Analytics to Better Understand Medicaid Populations with Serious Mental Illness,” Accessed November 29, 2022, [Weblink](#).
- Robert M. Goerge, Emily R. Wiegand, Emma K. Monahan, Leah Gjertson, “Exemplary Data Use by State TANF Agencies: Beyond Routine Reports and Analyses,” U.S. Department of Health & Human Services, Office of Planning, Research & Evaluation, August 2022, [Weblink](#).
- Zoë Neuberger and Lauren Hall, “WIC Coordination With Medicaid and SNAP,” Center on Budget and Policy Priorities, November 14, 2022, [Weblink](#).

