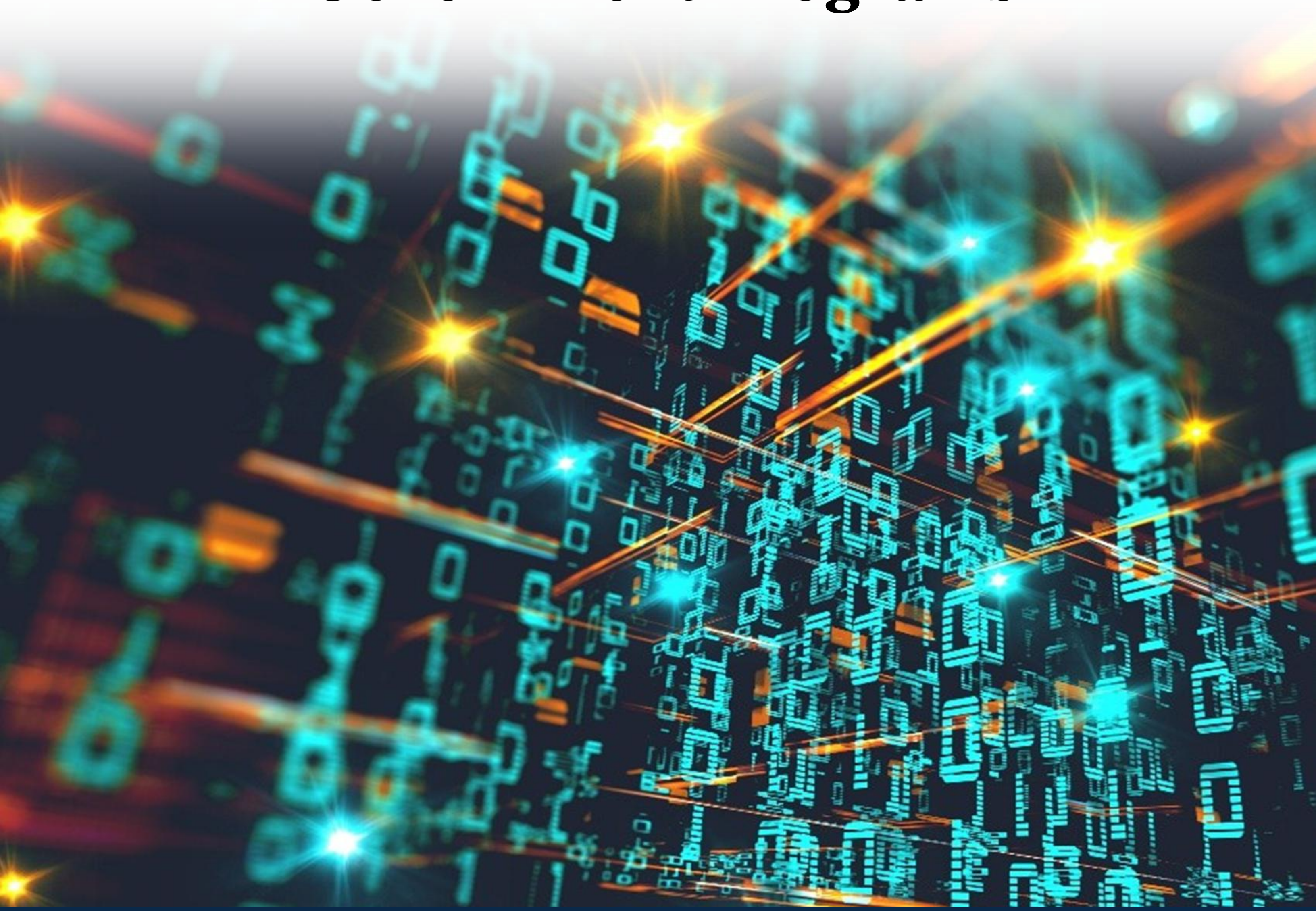
A Research Paper by the

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

for the Program Integrity Alliance

Balancing Data Sharing and Privacy to Enhance Integrity and Trust in Government Programs



Program Integrity Alliance

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION®

March 2025

This page is intentionally left blank.

March 2025

A Research Paper by the

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

for the Program Integrity Alliance

Balancing Data Sharing and Privacy to Enhance Integrity and Trust in Government Programs

NATIONAL ACADEMY OF
PUBLIC ADMINISTRATION®

Study Team
Brenna Isman, *Director of Academy Studies*
Chloe Yang, *Project Director*
Jesse Roth, *Senior Advisor*
Jonathan Garcia, *Research Analyst*
Jillian McGuffey, *Research Analyst*
Brad Riley, *Senior Research Associate*
Coleman Stallworth, *Senior Research Associate*

National Academy of Public Administration

1600 K Street, NW
Suite 400
Washington, D.C. 20006
www.napawash.org

March 2025
Printed in the United States of America
Academy Project Number: 22908

Cover Photo Source: Microsoft Stock Images.

About the Academy

The National Academy of Public Administration is an independent, nonprofit, and non-partisan organization established in 1967 and chartered by Congress in 1984. It provides expert advice to government leaders in building more effective, efficient, accountable, and transparent organizations. To carry out this mission, the Academy draws on the knowledge and experience of its over 1,000 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as prominent scholars, career public administrators, and nonprofit and business executives. The Academy helps public institutions address their most critical governance and management challenges through in-depth studies and analyses, advisory services and technical assistance, congressional testimony, forums and conferences, and online stakeholder engagement. Learn more about the Academy and its work at www.NAPAwash.org.

This page is intentionally left blank.

Foreword

Improper payments and fraud have been a long-standing, significant challenge in the federal government, undermining the integrity of federal programs and eroding public trust. In an era defined by rapid technological advancements and increased reliance on digital infrastructure, data plays a crucial role in detecting and preventing improper payments and fraud. The need for greater interagency collaboration and data-driven decision making has never been more critical. However, as this paper underscores, the evolving landscape of data governance introduces complex legal, operational, and ethical considerations that demand a well-thought-out nuanced approach.

The Program Integrity Alliance contracted with the National Academy of Public Administration (the Academy) to conduct a study to examine the inherent tensions between increased data sharing and protecting data privacy. The Academy has long been committed to strengthening governance and public administration through independent, nonpartisan expertise. Additionally, one of the Academy's 12 Grand Challenges in Public Administration is *Ensuring Data Security and Privacy Rights of Individuals*. In developing thought leadership for this Grand Challenge, the Academy has conducted research, written reports, and convened events on data security and privacy.

This paper examines the benefits and privacy challenges associated with data sharing across government programs in the context of program integrity and fraud prevention. It presents key findings and recommendations to bridge the gap between enhanced data accessibility and robust privacy safeguards and reflects focused research, engagement with key stakeholders, and an analysis of best practices to identify actionable solutions to strengthen data sharing and protect data privacy.

We appreciate the government officials and subject matter experts who contributed their insights and expertise to this effort. Their valuable perspectives have informed a comprehensive approach to strengthening data-sharing mechanisms while upholding privacy standards. Additionally, I would like to extend my sincere appreciation to the dedicated Study Team at the Academy.

As agencies continue to navigate the complexities of data governance, this paper serves as an essential resource for fostering collaboration, mitigating risks, and reinforcing the integrity of government programs. By embracing a strategic and transparent approach to data sharing, we can enhance the effectiveness of public administration and ensure that government services remain efficient and trustworthy.

James-Christian Blockwood
President and Chief Executive Officer
National Academy of Public Administration

This page is intentionally left blank.

Table of Contents

Acronyms and Abbreviations

Acronym or Abbreviation	**Definition**
Academy	National Academy of Public Administration
CARES	Coronavirus Aid Relief and Economic Security Act
CDO	Chief Data Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CMA	Computer Matching Agreement
CMS	Centers for Medicare and Medicaid Services
DNP	Do Not Pay
EDUCATION	Department of Education
FERPA	Family Educational Rights and Privacy Act
FUTURE	Fostering Undergraduate Talent by Unlocking Resources for Education
GAO	Government Accountability Office
GDPR	General Data Protection Regulation
HFPP	Healthcare Fraud Prevention Partnership
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IDR	Income-Driven Repayment
IRS	Internal Revenue Service
NDNH	National Directory of New Hires

NFD	National Fraud Database
NSDS	National Secure Data Services
NSF	National Science Foundation
OIG	Office of Inspectors General
OMB	Office of Management and Budget
PACE	Pandemic Analytics Center of Excellence
PHD	Public Health Data Warehouse
PII	Personally Identifiable Information
PRAC	Pandemic Response Accountability Committee
ROC	Recovery Operations Center
SBA	Small Business Administration
SORN	Systems of Records Notice
SSA	Social Security Administration
TTP	Trusted Third Party
UI	Unemployment Insurance

This page is intentionally left blank.

Section 1: Introduction

Improper payments and fraud are significant problems in the federal government because they erode public trust and waste taxpayer money. According to the Government Accountability Office (GAO), improper payments are defined as payments that "should not have been made or that were made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements."[1] Improper payments arise from various causes, including unintentional errors, insufficient documentation, and fraud and abuse.[2] The federal government is estimated to lose between $233 billion to $521 billion every year to fraud.[3] In addition, the estimated amount of federal improper payments was $236 billion in FY 2023.[4] Reducing improper payments and combating fraud is essential for protecting federal funds and maintaining public confidence in federal data systems.

Government programs have become more interconnected and reliant on data, and there is a growing recognition of the role of data in preventing improper payments and combating fraud. The government is exploring various ways to leverage technology and data analytics to detect and prevent misspending and fraud.

The increasing digitalization of government services has amplified the tension between data sharing and privacy concerns. Integrating systems and sharing data across programs can simplify data access and enhance service efficiency; however, this integration also brings up issues regarding the exposure of sensitive personal information to potential misuse, breaches, or unauthorized access. Finding a solution that balances effective data sharing with privacy protections is crucial for expanding data sharing and maintaining public trust.

1.1 Study Scope

The Program Integrity Alliance—a non-profit initiative promoting data-driven, evidence-based integrity, and fraud prevention in government—contracted with the National Academy of Public Administration (the Academy) to conduct a study to address the inherent tensions between increased data sharing and protecting individual privacy rights in the context of program integrity and fraud prevention. The study explored how government agencies can expand data-sharing initiatives to enhance fraud prevention and program efficiency without compromising privacy. Key research questions included:

- What are the benefits of data sharing in improving program integrity and preventing fraud?
- What are the privacy challenges associated with data sharing in federal government programs in the context of program integrity and fraud prevention?

[1] U.S. Government Accountability Office, *Improper Payments: Key Concepts and Information on Programs with High Rates or Lacking Estimates,* July 2024, p. 2. GAO-24-107482.
[2] Ibid.
[3] U.S. Government Accountability Office, *Fraud & Improper Payments*, https://www.gao.gov/fraud-improper-payments.
[4] Ibid.

- What potential legal, regulatory, or policy changes are needed to protect privacy while strengthening and expanding data-sharing initiatives across government agencies?

1.2 Study Methodology

The study was conducted from December 2024 through February 2025. The Study Team carried out primary and secondary research to develop findings and recommendations. As background research, the Study Team collected and reviewed a variety of documents, including primary privacy laws, regulations, policy documents, and previous reports and reviews. Additionally, the Study Team gathered information through semi-structured interviews with knowledgeable individuals during the two months of data collection. Interviewees include government officials, congressional staff, privacy law experts, fraud prevention experts, and selected Academy Fellows. All interviews were conducted on a not-for-attribution basis. Appendix A provides a comprehensive list of the individuals interviewed by the Study Team.

To acquire a broader perspective on key issues, the Study Team also conducted two roundtables that gathered insights from thought leaders in data sharing and privacy, legal experts, and public administration professionals. These roundtables provided a forum for experts to discuss emerging challenges and identify practical solutions that consider both data-sharing needs and privacy concerns. Roundtable participants are listed in Appendix B.

Section 2: Benefits of Data Sharing in Enhancing Program Integrity and Fraud Prevention

Government databases are a collection of electronic records and information managed by government entities and generally contain data like citizen records, financial information, legislative documents, public health statistics, and census data. Government databases are designed to ensure data accuracy, integrity, security, and accessibility for authorized users. The purpose of these databases is for policy making, public service delivery, fraud detection and prevention, law enforcement, and national security.

Federal agencies have increasingly leveraged data and interagency data-sharing agreements to enhance program integrity and increase fraud detection and prevention capabilities. Integrating and cross-referencing data sets increases the identification of inconsistencies and fraudulent patterns that might otherwise remain undetected within information silos. Expanding access to data is crucial in enhancing fraud prevention and detection efforts by enabling agencies to identify, analyze, and respond to emerging threats with greater accuracy. Increasing interagency data sharing breaks down the limitations of siloed information. In addition, data sharing helps improve data quality and detect errors by allowing multiple parties to cross-check information and validate data accuracy.

2.1 Oversight Bodies Have Benefited from Data Sharing

Key oversight bodies, such as GAO and Offices of Inspectors General (OIGs), benefit from utilizing data sets through targeted waivers and exemptions from specific privacy regulations, proving that greater access to data allows more comprehensive audits, compliance assessments, and systemic vulnerability identification within federal programs. These mechanisms reinforce accountability and transparency while ensuring enhanced data-sharing initiatives do not compromise individual privacy rights or statutory protections.

In its report titled “Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely Between $100 Billion and $135 Billion,”[5] GAO used data from multiple agencies to identify waste, fraud, and abuse in unemployment insurance (UI) programs during the COVID-19 pandemic. To estimate the extent of fraud, GAO reviewed data from the Department of Labor, selected and analyzed a sample of payments, and matched these samples to other federal databases. Additionally, GAO reviewed data on state-reported overpayments, recoveries, and waivers and interviewed officials from 14 states selected based on fraud risk and other factors. By integrating data from numerous sources, GAO produced a comprehensive estimate of fraud within UI programs during the pandemic, highlighting the importance of interagency data sharing in identifying and mitigating waste, fraud, and abuse.

2.2 Data Sharing Has Helped Prevent Fraud

Interagency collaboration using a number of data sets has demonstrated the benefit of cross-referencing information with authoritative data sources, such as Social Security Administration (SSA) records, to identify fraudulent claims and mitigate financial losses. A key example is the U.S. Department of the Treasury's Do Not Pay (DNP) Business Center, a centralized resource designed to help federal agencies prevent, identify, and recover improper payments. With access to various data sources, the DNP assists agencies in verifying beneficiary eligibility and ensuring that federal funds are disbursed correctly. The DNP Business Center has access to multiple databases and provides data-matching services to verify the eligibility of vendors, grantees, loan recipients, or beneficiaries. The DNP Business Center also offers custom services, including deceased payee analyses, data quality integrity, business risk assessments, and cross-agency analyses.

The Consolidated Appropriations Act of 2021 granted Treasury temporary access to SSA’s full Death Master File for three years, effective December 2023. The DNP Business Center conducted a five-month pilot program utilizing SSA's Death Master File. This effort prevented and recovered over $31 million in improper payments to deceased individuals. The pilot, which began in December 2023, demonstrated enhanced detection capabilities, resulting in a 139% increase in death matches and improved data quality. Treasury officials project a net benefit of over $215 million during the three-year access period ending in December 2026.[6]

The opportunity costs of not sharing data are substantial. For example, the Pandemic Response Accountability Committee (PRAC) found “$5.4 billion in potential identity fraud associated with

[5] U.S. Government Accountability Office, *Agency Actions and Data Use in Workforce Diversity Efforts*, GAO-23-106696, September 2023, https://www.gao.gov/assets/gao-23-106696.pdf.

[6] U.S. Department of the Treasury, *"Treasury Department Announces Actions to Bolster Beneficial Ownership Transparency and Counter Illicit Finance,"* press release, December 22, 2023, https://home.treasury.gov/news/press-releases/jy2784.

69,323 questionable and unverified Social Security numbers."[7] According to GAO, the Small Business Administration (SBA) was not able to verify applicants' Social Security numbers, primarily due to the lengthy process of implementing an SSN verification agreement. PRAC stated that it could have significantly reduced identity theft if the SBA had access to SSA's data.[8]

2.3 Summary

In an era of increasingly sophisticated fraud schemes, data sharing is critical in safeguarding federal programs against waste, fraud, and abuse. By sharing data and using technologies, agencies can detect fraudulent activities more effectively and prevent improper payments. Beyond its role in fraud prevention, enhanced data-sharing mechanisms are beneficial for informing evidence-based policymaking and improving service delivery. By integrating and analyzing multiple data sets, agencies can identify service gaps, assess regional disparities in program access, and develop targeted interventions that address systemic inequities.

Section 3: Challenges and Recommendations

3.1 Overview: Tensions between Expanding Data Sharing and Protecting Data Privacy

The federal government increasingly relies on data and interagency data sharing to inform policy decisions, ensure program integrity, and enhance accountability. As discussed in Section 2, oversight bodies have benefited from data sharing. Laws grant oversight bodies broad access to agency data to detect and prevent waste, fraud, and abuse. For example, the Government Accountability Office (GAO) has statutory authority[9] to access agency records to support its role in evaluating federal programs and ensuring accountability. Similarly, the Inspector General Act of 1978 provides each Inspector General (IG) the authority to "have access to all records, reports, audits, reviews, documents, papers, recommendations or other material available to the agency."[10] Additionally, the Inspector General Empowerment Act of 2016 exempts IGs from the statutory requirement to establish computer matching agreements with other agencies for data-matching activities when conducting an audit, evaluation, or investigation. These laws demonstrate how data access carveouts can be provided to facilitate fraud prevention and address waste and abuse in the federal government.

The growing dependence on data exacerbates the tension between the need to share information across agencies and the responsibility to protect privacy. The government collects huge amounts of personal financial, health, and other sensitive information from the public on a daily basis and has the responsibility to keep the information safeguarded from abuse. However, the data infrastructure in both the public and private sectors is vulnerable to attacks, and the threat of

[7] U.S. Government Accountability Office, *GAO-02-1058: Information Management Selected Agencies' Handling of Personal Information*, September 2002, p. 12, https://www.gao.gov/assets/gao-02-1058.pdf.
[8]Ibid.
[9] U.S. Code, 31 U.S.C. § 716, https://www.law.cornell.edu/uscode/text/31/716.
[10] U.S. Congress, *the Inspector General Act of 1978*, Public Law 95-452, enacted October 12, 1978.

exposure to data breaches is significant. While data sharing can enhance transparency and program integrity, many agencies approach it cautiously, concerned about legal risks, compliance burdens, and potential misuse.

A complex web of privacy laws and regulatory requirements further complicates data-sharing efforts. While these safeguards protect sensitive information, they require agencies to follow detailed administrative processes before sharing data, adding bureaucratic burdens that slow or discourage collaboration. On the one hand, laws such as the Privacy Act of 1974 ensure that sensitive personal data are safeguarded against unauthorized disclosure. On the other hand, these same laws can limit government agencies' ability to share data for legitimate and beneficial purposes, including strengthening program integrity and preventing fraud.

Differing interpretations of privacy laws add another layer of inconsistency, making it even more challenging to establish standardized data governance practices. Restrictive policies and siloed data management practices often limit collaboration, creating inefficiencies and missed opportunities for more effective governance.

Table I: Tensions between Data Sharing and Data Privacy

Data Sharing	Data Privacy
• Government programs have become more interconnected and reliant on data. Effective data sharing between agencies is key to reducing improper payments and fraud. • Data sharing enhances fraud detection and prevention efforts and increases the identification of inconsistencies and fraudulent patterns. • Oversight bodies have benefited from data sharing. • Legislations afford some government agencies access to data to protect program integrity.	• Data infrastructure is vulnerable to attacks, and the threat of exposure to data breaches is significant. • There is a growing concern about the potential exposure of private information. • Privacy laws and regulations protect data privacy but require agencies to follow detailed administrative processes, hindering agencies' ability to share data for legitimate purposes. • Restrictive policies and siloed data management often limit collaboration.

This section examines the legal, regulatory, and structural challenges associated with the government's data sharing and privacy approach. The discussion provides an overview of key legislative frameworks that govern data use, highlighting the complexities agencies must navigate when balancing information sharing with privacy protection. This section also explores how agencies' data management practices, restrictive policies, and lengthy compliance processes contribute to the tension between transparency and data privacy. Understanding these challenges is critical to evaluating how government agencies can responsibly share data while maintaining public trust.

3.2 Legal Barriers and Implementation Challenges

Government agencies operate within a complex legal framework that governs how data is collected, maintained, and shared. While data sharing can enhance program effectiveness, support evidence-based policy making, and improve fraud prevention, agencies must navigate multiple laws that impose restrictions to protect individuals' privacy and ensure proper data stewardship.

Overview of Primary Legislative Requirements

Privacy laws establish procedural safeguards, define permissible uses of data, and create oversight mechanisms to ensure compliance. However, they also contribute to the complexity of interagency data sharing, often requiring lengthy approvals, legal justifications, and extensive administrative processes. Table II below provides an overview of primary privacy laws.

Table II: Primary Legislative Requirements

Major Privacy Laws	
Law	**Key Requirements**
Privacy Act of 1974	• Establishes a framework for how federal agencies collect, maintain, and disseminate Personally Identifiable Information (PII). • Requires consent before disclosure of personal data, complicating legitimate efforts to share data between agencies.[11]
Computer Matching and Privacy Protection Act of 1988	• Regulates use of computer matching programs, requiring written agreements and due process for individuals whose data is matched. • Limits the ability to share data across agencies even when it could aid analysis or policy development
E-Government Act of 2002	• Promotes electronic government information and services through digital tools. • Requires Privacy Impact Assessments to identify potential risks and implement measures to mitigate them before collecting, sharing, or using PII in a new digital system, adding additional review and approval layers.[12]
Examples of Sector-specific Privacy Laws	
Law	**Key Requirements**
HIPAA (Health Insurance Portability and Accountability Act)	• Regulates how health records can be shared, ensuring health data is only disclosed for permitted purposes.
FERPA (Family Educational Rights and Privacy Act)	• Protects student records and restricts their disclosure by educational institutions and federal agencies.
Internal Revenue Code Section 6103	• Restricts disclosure of tax return information outside the IRS, except under specific legal authorizations.

These laws serve critical functions in protecting personal information but create a fragmented landscape in which different agencies operate under various legal obligations, making interagency data sharing particularly challenging. Understanding these legal requirements is essential for

[11] U.S. Department of Justice, *Privacy Act of 1974*, https://www.justice.gov/opcl/privacy-act-1974.

[12] U.S. Congress, *Public Law 107-347—E-Government Act of 2002*, December 17, 2002, https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

assessing the challenges agencies face in balancing privacy protection with the need for improved data accessibility.

Importance of Privacy Laws and Regulations

Privacy laws and regulations are a fundamental safeguard in ensuring government agencies collect, manage, and share data responsibly. These laws establish a structured framework for responsible data handling and protect individuals' rights by preventing unauthorized access to personal information and reducing the risk of data misuse. By establishing clear data collection, use, and disclosure guidelines, privacy laws reinforce government agencies' ethical and legal responsibilities, ensuring that personal information is handled with care, security, and accountability.

A key role of privacy laws and regulations is maintaining public trust in government institutions. In an era where data collection and digital records are expanding, individuals must feel confident that their personal information is protected. When citizens trust that their data is secure, they are more likely to engage with government services, participate in public programs, and share necessary information without fear of misuse.

Varying Interpretations of Privacy Laws

Some data-sharing challenges arise from inconsistent interpretations of privacy laws across government agencies. Agencies interpret laws in ways that support their specific missions. Unless there is mission alignment, interpretations are likely to vary. Within the same context, the interpretation of what and how data can be shared varies, and there may also be different interpretations or "readings" of laws within the same agency. Thus, certain agencies are very restrictive in how they share their data, while others may be less restrictive even though the data and environment may be similar or, in some cases, identical. For example, based on its interpretation of relevant laws, the Department of Health and Human Services (HHS) held that the statute did not authorize HHS to share the National Directory of New Hires (NDNH) data with GAO. HHS's view was that this specific statute limited GAO's broad data access authority.[13] It required the enactment of a statute that specifically grants GAO the authority to access the NDNH data.

In addition, agencies' interpretations of privacy laws depend on the background and experience of the attorney. Individual agencies' different readings of privacy laws result in different data systems and standards, leading to lengthy, tedious data-sharing negotiation processes and creating data "silos" that make cross-agency data sharing difficult. These differing legal interpretations may be addressed partly through discussions when developing data agreements. Further guidance from Congress or the Office of Management and Budget (OMB) may help narrow the legal interpretations.

Implementation Challenges

Implementing privacy laws can be challenging for organizations due to a number of factors. Federal agencies must navigate an increasing patchwork of data protection legislation and

[13] U.S. Code, 31 U.S.C. § 716, https://www.law.cornell.edu/uscode/text/31/716.

regulations. This environment is dynamic, complex, and influenced by several factors, including: understanding and keeping up to date with relevant laws and regulations; having enough staff and resources to address the requirements of laws and regulations; managing the transfer of data across agencies or states; responding to requests from individuals about their data; protecting against data breaches and cyberattacks; not having visibility into how the data is collected, used, and shared; and not having effective collaboration between those sharing the data.

SORN Requirements

One significant process challenge under the Privacy Act is the requirement for agencies to publish a system of records notice (SORN) in the Federal Register to provide public notice of their systems of records. It further gives individuals the right to review, correct, or amend their records. In addition, it requires agencies to comply with statutory norms for collecting, maintaining, and disseminating records. In many cases, it requires a lengthy, labor-intensive, and complex process to fulfill the requirements of the Privacy Act.

Federal agencies publish a SORN in the Federal Register upon establishment and/or modification of a system of records. A SORN describes what information is collected and maintained in the system, how the information is stored and used, and the procedures by which individuals can request access to or correct information about them. A SORN includes the routine uses for which information can be disclosed. A SORN also identifies the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, and the routine uses to which records are subject. Agencies' processes for preparing and drafting a new SORN can vary significantly. It generally requires a lengthy period to establish a SORN, primarily due to challenges related to the coverage of the SORN. Questions often arise about data access authorities and the scope of the system of records.

Agencies are required to add a new routine use to the SORN when sharing data for a purpose that is different from the one for which it was originally collected. To modify the routine use, agencies need to prepare documentation explaining the purpose of the proposed modification, submit it to OMB and Congress, and publish the notice in the Federal Register for public comment. Interviewees noted that the process used to add a new routine use, in theory, is faster than the one for publishing a new SORN.

Computer Matching and Privacy Protection Act

Another legislative requirement mentioned previously that may create a challenge for data sharing is the "Computer Matching and Privacy Protection Act." The Act amended the Privacy Act of 1974 and established additional procedural privacy safeguards by requiring Federal agencies to enter into written agreements (i.e., computer matching agreements (CMAs)) with other agencies or non-Federal entities before disclosing records for use in computer matching programs. In addition to creating/updating SORNs, it requires significant time and effort to address its provisions, including:

- Publish a Federal Register notice of the establishment or the revision of such programs and provide notice to Congress and the Office of Management and Budget.

- Establish a Data Integrity Board to oversee and coordinate the implementation of this Act.
- Demonstrate that the proposed program is cost-effective through a cost-benefit analysis before establishing a matching program.
- Report to Congress on information obtained from reports from the various Boards.
- Require the Director to provide guidelines, regulations, assistance, and oversight regarding the implementation of this Act.
- Require the Office of the Federal Register annually to publish rules promulgated and agency notices on records maintained on individuals.

According to interviewees, it may take more than a year to go through the entire process. The arduous process has presented significant hurdles in expanding data-sharing efforts to support fraud prevention. Take the onboarding process of the Treasury's DNP as an example: after submitting applications, an agency may need to go through the process of updating applicable SORNs if they do not already include program integrity and fraud prevention as a routine use. In some instances, a CMA is required, which involves initiating the CMA, conducting a cost-benefit analysis, and finalizing the CMA after review and approval by both agencies' Data Integrity Boards. Agencies are required to update their CMAs, at a minimum, every three years. Interviewees noted that some agencies dropped out of the DNP program because they failed to update their CMAs. Under the Payment Integrity Information Act of 2019, DNP's authorizing legislation, the head of the agency operating the DNP working system, in consultation with OMB, may waive the CMA requirements as part of the DNP initiative.[14] However, this waiver authority has been utilized somewhat infrequently to date, and would benefit from the issuance of guidance from OMB.[15]

Recommendations

> ***To facilitate data sharing among federal agencies to improve program integrity and combat fraud, OMB should issue guidance (Memoranda) that agencies include fraud prevention and program integrity as routine use in each of the agencies' SORN.***

OMB has the authority under the Privacy Act to issue guidance to executive branch agencies on how to implement statutory requirements. As an example, OMB issued a memo titled "Preparing for and Responding to a Breach of Personally Identifiable Information" in 2017, requiring agencies to incorporate two routine uses into each of the agencies' SORNs.[16] The purpose of this memo was to reduce data-sharing barriers and enable agencies to manage large breaches that

[14] U.S. Congress, *Payment Integrity Information Act of 2019*, Public Law 116-117, enacted March 2, 2020, https://www.congress.gov/116/plaws/publ117/PLAW-116publ117.pdf.

[15] On March 25, 2025, the Trump Administration issued an Executive Order, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*, directing the Secretary of the Treasury to exercise the authority in 31 U.S.C. 3351 *et seq* to waive the CMA requirements (5 U.S.C. 552a(o)).

[16] U.S. Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information*, Memorandum M-17-12 (January 3, 2017), https://www.commerce.gov/sites/default/files/opog/omb_m-17-12.pdf.

implicate multiple agencies more effectively. Similar guidance from OMB would help streamline the process and facilitate data sharing to detect and prevent fraud and improper payments.

On March 25, 2025, the Trump Administration issued an Executive Order (EO), *Protecting America's Bank Account Against Fraud, Waste, and Abuse*, directing agency heads to review and modify their relevant SORNs to include a routine use that allows for the disclosure of records to the Treasury for the purposes of detecting and preventing improper payments and fraud. This directive could provide a precedent for government-wide data sharing.

Federal agencies should work with Congress to enact Special Authorities or Statutory Exemptions to address data sharing between agencies, focusing on exceptions for designated areas such as program integrity and fraud prevention.

Interviewees highlighted some examples of how privacy laws can be limited when there is a valid reason. For example, the Inspector General Empowerment Act amends the Inspector General Act of 1978 to exempt inspectors general (when they are conducting an authorized audit, investigation, inspection, evaluation, or review) from information privacy protections that require agreements between agencies for computerized comparisons of automated federal records systems under the Computer Matching and Privacy Protection Act of 1988.

An example of how sector-specific laws might be changed to facilitate data sharing is the case where the Internal Revenue Service (IRS) privacy laws (i.e., the Internal Revenue Code) hindered the Department of Education (Education) from identifying potential fraud in one of its programs. To ease the burden of federal student loans, borrowers can apply for Income-Driven Repayment (IDR) plans. The plans use borrowers' taxable income and family size to determine an affordable payment rate. However, as discussed earlier, the Internal Revenue Code Section 6103 prevents tax return information from being disclosed outside the agency. GAO conducted a study and recommended that Education request and obtain data (from the IRS) to verify income information for borrowers who report zero income on IDR plan applications to identify and address possible fraudulent activity. In December 2019, Congress passed the Fostering Undergraduate Talent by Unlocking Resources for Education (FUTURE) Act, which amends the Internal Revenue Code to allow for direct data sharing between the IRS and Education.

HIPAA offers another example of statutory exemptions—specific rules associated with using and sharing sensitive information—to support fraud prevention. As discussed in previous sections, HIPPA establishes federal standards to safeguard sensitive health information. In the HIPPA framework, a covered entity has the authority to disclose PHI for the purposes of fraud and abuse detection without an individual's authorization.

It is important to recognize the potential risks of granting special authorities or statutory exemptions. Interviewees expressed concern that special data access authorities/statutory exemptions are granted only for the purpose of expediency and provide avenues to bypass privacy requirements. It is essential that the flexibility provided does not undermine the legal framework that safeguards data privacy and public trust and that accountability mechanisms are in place to prevent the circumvention of privacy protections.

Individual agencies should take the lead in working with Congress to obtain special authorities or statutory exemptions in support of program integrity and fraud prevention. This approach would allow Congress and other stakeholders to examine the challenges facing each agency and carefully define the scope of the special authorities or exemptions to ensure that data are truly used to reduce and prevent fraud, waste, and abuse.

3.3 Data Management Framework

A fragmented data management framework, where agencies collect and manage data in silos, is identified by interviewees as a root cause of the data-sharing challenges in the government. Vast amounts of data are scattered across hundreds of disconnected systems within the federal government. Fragmented data management limits the federal government's ability to proactively address program vulnerabilities and prevent fraud. Fraudsters typically do not focus on just one government program but target multiple programs to maximize gains. It is critical to look across a wide range of programs and agencies to uncover patterns and identify irregularities that may point to improper payments or fraud.

Costs of Data Sharing

The costs of sharing data have been identified as a key factor that leads to the fragmented data management framework in the federal government. Agencies collect data to fulfill their missions, but there is no strong incentive for an agency to share data with other agencies. It is necessary to acknowledge that the costs of sharing data securely are significant. Some interviewees noted that many agencies view data sharing as an "unfunded mandate" and are hesitant to share data unless required by law. For example, SSA is authorized to collect death data from states to administer social security benefits programs and share death data with a limited number of federal agencies. According to SSA officials, death data collection is critical to SSA's core mission; however, sharing death data does not support SSA's mission and represents a substantial workload.[17]

Under the fragmented data management framework, data sharing is often seen as a compliance task, and as a result, some agencies develop very restrictive data-sharing policies and are reluctant to take time to understand the requirements set by privacy laws and regulations, assess potential risks, and work through statutory barriers, but cite "privacy" as a reason for not sharing data.

Agencies would be more willing to share data as they see benefits. Interviewees said that financial institutions invest millions of dollars into data sharing and fraud prevention because tracking the "return on investment" (e.g., the amount of financial fraud reduced as a result of the investment) is relatively straightforward. However, making a similar value proposition in the government is not easy. The connection between the perceived benefits and resources required to share data can be challenging to measure.

Leadership Commitment

The absence of strong, consistent leadership in the executive branch is another factor that contributes to the fragmented data management framework. The Evidence Act provides the legal

[17] National Academy of Public Administration, *A Report to Congress on Sources of and Access to State Death Data*, July 2022, https://s3.us-west-2.amazonaws.com/napa-2021/SSA-State-Death-Data.pdf.

framework for managing government data and utilizing data in decision making. The Act establishes the role of the agency's Chief Data Officer (CDO).[18] Under the Evidence Act, CDOs oversee Information Resource Management, including enhancing data integration and quality. Some interviewees pointed out the lack of clarity around the authorities of CDOs versus CIOs and suggested elevating the CDO position and enhancing the authorities and qualification requirements of CDOs to support data sharing and integration within the federal government.

The support of agency leaders is critical to facilitating data sharing across the federal government and breaking through cultural barriers and information silos. Interviewees noted that some agencies are averse to considering potential fraud risks — "we have no fraud"— and pointed to the lack of commitment from agency leaders to integrate data/evidence into decision making. Interviewees stressed the need to embrace a more data-driven mindset and adopt a "trust but verify" approach to preventing improper payments and fraud.

Recommendation

> ***To drive cultural change and encourage data sharing, Congress could mandate the creation of a centralized data platform to support program integrity and fraud prevention.***

A common theme that emerged from roundtable discussions and interviews is the value of creating a centralized data platform for secure data sharing and data analysis. A centralized data platform would have access to a variety of federal and state agency data sets and provide data analytics services to authorized participants to support program integrity and fraud prevention.

Protect Data Privacy and Security

A major concern about the centralized data management model discussed by interviewees is the potential risks to data privacy and the security of the platform. This platform would be subject to relevant privacy laws and regulations and would need to negotiate data-sharing agreements with all participating agencies. The development of data-sharing agreements is often time-consuming. However, the centralized data management approach would be more efficient and reduce duplicative efforts compared to the current model, where each agency independently negotiates its data-sharing agreements with other agencies and establishes policies, processes, and systems to receive and maintain data.

It is critical to implement appropriate measures against security breaches and protect private information. Privacy-enhancing technology offers a way forward, allowing for greater data sharing with tight control to ensure compliance with privacy laws and regulations. Roundtable participants emphasized the difference between "data shared" and "data shown." Data query enables users to access specific information without transferring the whole data set, improving efficiency and security for various analytical purposes.

The primary technology used to protect data sharing is encryption, which converts data into a coded format that can only be deciphered with the correct key, ensuring that only authorized

[18] U.S. Congress**.** *Foundations for Evidence-Based Policymaking Act of 2018*, Public Law 115-435, 115th Cong. (January 14, 2019). https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf.

parties can access sensitive information when shared. Other key technologies available to facilitate data sharing by providing a secure environment include:

- Firewalls: The initial security layer in a system. It is designed to keep unauthorized sources from accessing enterprise data.
- Access Control: Limits who can access sensitive data through mechanisms like passwords, biometrics, and user permissions.
- Role-based access control: Assigns specific permissions to users based on their roles within an organization, further restricting data access.
- Multi-factor authentication: Requires users to provide multiple forms of identification, like a password and a code sent to their phone to access data, enhancing security.
- Data masking: Replaces sensitive data with placeholder values while preserving the data structure for testing purposes.
- Data anonymization: Removes personally identifiable information from data to protect privacy.
- Secure data exchange platform: Using protocols like Hypertext Transfer Protocol Secure (HTTPS) to encrypt data during transmission.
- Data loss prevention: Monitors data flows to identify and block potential data breaches.

These are just a few of the technological measures available to make data sharing easier through security. The technology utilized is dictated by the type and content of the data being managed. Taken together, the data security technologies available can under most circumstances allow for secure data sharing and provide assurance for the data owner that the data will be protected and not accessed by unauthorized persons. As technology advances these measures will become even more effective.

A key element of the centralized data platform is establishing policies and processes for vetting participants. Only authorized members would have access to the data and data analytics provided by this centralized data platform. Data access classification is a process for vetting participants by categorizing data based on a number of factors and assigning it to a security level. Data is categorized based on factors such as sensitivity, type, and desired user access. Data classification helps prevent data breaches, hacks, and cyberattacks, aids organizations in complying with laws and regulations, and assists organizations in prioritizing resources. Data classification can be performed manually, automatically, or a combination of both.

Leverage Existing Initiatives

A centralized data platform is not new in the federal government. The Study Team has identified several examples of centralized data services at the federal and state levels. These examples illustrate the potential of a centralized data platform, demonstrating how it can enhance efficiency, reduce duplicative efforts, and ensure data security and privacy. It is important for Congress to build on existing frameworks and leverage the promising practices and lessons learned from previous initiatives.

The Treasury's DNP system serves as a model for utilizing various data sources to reduce improper payments. As discussed in Section 2, the DNP has access to multiple public or restricted data sources, serving as a "data source aggregator,"[19] and provides a variety of data matching and analytics services to support agency programs in identifying and mitigating improper payments. The DNP has implemented an enrollment process and policies to verify agencies' eligibility to use the DNP portal and protect the privacy of information.[20]

Interviewees highlighted several examples of centralized data platforms in the oversight community. For example, to carry out its oversight responsibilities, the Recovery Board established the Recovery Operations Center (ROC), a central data analytics service to support fraud detection and prevention and assist the oversight communities. The ROC obtained access to 24 data sets, including government, law enforcement, commercial, and open-source data.[21] The ROC was widely praised by stakeholders. According to GAO, the ROC provided significant data analytical support to the oversight community.[22] GAO stated that Congress should consider directing the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to "develop a legislative proposal to reconstitute the essential capabilities of the ROC to help ensure federal spending accountability."[23]

Modeled after the ROC, the Pandemic Analytics Center of Excellence (PACE) provides another example of a centralized data analytics platform. The PRAC was created as a special committee within the CIGIE under the Coronavirus Aid Relief and Economic Security (CARES) Act of 2020[24] to prevent and detect waste, fraud, and abuse of the federal government's COVID-19 spending, which totals over $5 trillion.[25] The PRAC established the PACE to enable data sharing and data analytics across the IG community and law enforcement. The PACE has access to more than 50 data sets from a variety of public, non-public, and commercial sources[26], each of which has its own requirements regarding data use and data sharing. In 2024, the PACE completed the implementation of the Analytic Center Pilot to provide risk analytics services. This pilot, comprised of government data sources, provided various dashboards that highlighted risk indicators from the data sources. This pilot was recognized by users as the "gold standard" for interagency data sharing.[27] The PACE adopts a multi-layered approach to protecting data security, including robust encryption, rigorous access control, regular security audits, employee data

[19] National Academy of Public Administration, *A Report to Congress on Sources of and Access to State Death Data*, July 2022, https://s3.us-west-2.amazonaws.com/napa-2021/SSA-State-Death-Data.pdf.
[20] Ibid.
[21] U.S. Government Accountability Office, *GAO-15-814 Federal Spending Accountability Preserving Capabilities of Recovery Operations Center Could Help Sustain Oversight of Federal Expenditures*, September 2015, https://www.gao.gov/assets/gao-15-814.pdf.
[22] Ibid.
[23] Ibid. Pg. 24
[24] U.S. Congress, *Public Law 116-136—Coronavirus Aid, Relief, and Economic Security (CARES) Act*, March 27, 2020, https://www.congress.gov/116/plaws/publ136/PLAW-116publ136.pdf.
[25] U.S. Congress, *H.R. 748—Coronavirus Aid, Relief, and Economic Security (CARES) Act*, 116th Cong., enacted March 27, 2020, https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.
[26] Pandemic Response Accountability Committee, *Pandemic Analytics Center of Excellence*, https://pandemicoversight.gov/spotlight/pandemic-analytics-center-excellence.
[27] Pandemic Response Accountability Committee, *Semiannual Report to Congress: April 1, 2024 – September 30, 2024*, https://www.pandemicoversight.gov/media/file/report-congress-april-through-september-30-2024pdf.

security training, and comprehensive incident management programs.[28] Interviewees noted that both ROC and PACE obtained access to federal data sets through MOUs and had to address the issues related to SORNs (a more detailed discussion of SORN issues appears in Section 3.2); however, they are exempted from the procedural requirements under the Computer Matching Act because of the IG authorities.

Roundtable participants discussed data-sharing practices in the federal healthcare sector. The Healthcare Fraud Prevention Partnership (HFPP) provides an example of establishing a Trusted Third Party (TTP) that can aggregate data from multiple agencies/entities, securely maintain the data, and conduct analytics. HFPP was established to facilitate data sharing between healthcare entities to identify and prevent fraud.[29] Overseen by the Centers for Medicare and Medicaid Services, HFPP is operated by a federal contractor—the TTP—and currently is comprised of more than 300 partners, including federal, state, and local agencies, private payers, law enforcement agencies, and associations.[30] HFPP participating entities send healthcare claims data to TTP, which analyzes the data and identifies fraud schemes. HFPP has developed membership criteria and a process for reviewing membership applications. HFPP stores the data collected from participants in a data warehouse and has implemented "role-based access control" to ensure that sensitive data is only accessible to authorized users.

The National Secure Data Service (NSDS) exemplifies a government-wide data-shared service model. Authorized by the 2022 CHIPS and Science Act, the National Science Foundation (NSF) developed the NSDS Demonstration project to strengthen data linkage and support statistical activities. A key component of the NSDS Demonstration project is ensuring data privacy and confidentiality.[31] Only authorized individuals/entities have access to confidential data. The NSDS Demonstration project is exploring various ways, such as leveraging encryption techniques, using synthetic data, and using disclosure limitation methodologies to protect data privacy while expanding its access.[32]

Further, the Digital Accountability and Transparency Act (DATA) is an example of legislation that standardizes data to facilitate sharing across the Federal government. The Act is a law that mandates the U.S. government to establish standardized reporting systems for federal spending data, making it easily accessible and searchable for the public through a central website

[28] Michael E. Horowitz, *Statement of Michael E. Horowitz, Chair, Pandemic Response Accountability Committee, Inspector General, U.S. Department of Justice, before the U.S. House of Representatives Committee on Oversight and Accountability, Subcommittee on Government Operations and the Federal Workforce, concerning "Where Do We Go From Here? Examining a Path Forward to Assess Agencies' Efforts to Prevent Improper Payments and Fraud,* "September 10, 2024, https://www.pandemicoversight.gov/media/file/sept-10-testimony-prac-chair-michael-horowitz0pdf.

[29] Centers for Medicare & Medicaid Services, *About the Healthcare Fraud Prevention Partnership*, https://www.cms.gov/medicare/medicaid-coordination/healthcare-fraud-prevention-partnership/about.

[30] Centers for Medicare & Medicaid Services, *Healthcare Fraud Prevention Partnership*, https://www.cms.gov/medicare/medicaid-coordination/healthcare-fraud-prevention-partnership.

[31] National Center for Science and Engineering Statistics, *Privacy and Confidentiality—National Secure Data Service Demonstration Project*, https://ncses.nsf.gov/initiatives/national-secure-data-service-demo/privacy-confidentiality.

[32] Ibid.

(USAspending.gov), aiming to improve transparency and accountability in how taxpayer dollars are used across different government agencies. Interviewees noted that standardized data architecture would significantly improve data integrity and facilitate data sharing among agencies.

Roundtable participants and interviewees highlighted some centralized data-sharing initiatives at the state level. Massachusetts has established the Public Health Data (PHD) Warehouse that uses privacy-protected methods to connect person-level data across 27 state agencies and 38 data sources, including "vital records, public health, health care, social service, and justice."[33] The PHD provides data query services to authorized researchers and policy makers without sharing private information. This model links individual-level data temporarily for analysis behind a firewall without storing it in a shared database, and results are reported without identifying the individual.[34]

The Study Team's research also identifies some leading practices from other countries. For example, the UK is seen as a leader in data sharing and privacy. Cifas is a non-profit organization with a mission to reduce fraud and financial crime. Cifas' membership includes more than 750 organizations, including financial institutions, telecommunications, insurance, as well as some public sector organizations. An essential component of Cifas' anti-fraud initiatives is the National Fraud Database (NFD), which contains fraud risk data from member organizations and is the UK's largest fraud risk database. NFD enables real-time data sharing among its members and provides tools and analytics to allow members to identify fraud patterns and spot areas of improvement. NFD utilizes secure platforms and API integration to ensure efficient and secure data access. Cifas charges subscription fees to its members based on the size of the organization. Cifas members are required to follow the guidelines set forth in the NFD Handbook. The Handbook outlines eight Principles of use with accompanying guidance, including transparency, lawfulness, and integrity, to ensure data quality, protection, and lawful use.[35] In 2023, Cifas reported an estimated prevented fraud loss of £1.8 billion.[36]

There are some new initiatives to facilitate data sharing within the federal government. For example, the Trump Administration issued EO "Protecting America's Bank Account Against Fraud, Waste, and Abuse" *on* March 25, 2025*,* directing agencies to consolidate their core financial systems and adopt standard financial management solutions. These initiatives could provide context to inform the development of a comprehensive, centralized data platform.

[33] Jane Wiseman, *Case Study of the Massachusetts Public Health Data Warehouse and the use of data to address opioid overdoses*
, https://janewiseman.scholars.harvard.edu/sites/g/files/omnuum6041/files/janewiseman/files/massachusetts_public_health_data_warehouse.pdf.

[34] Ibid.

[35] CIFAS, *National Fraud Database*, https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database.

[36] Cifas, *National Fraud Database*, https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database.

Section 4: Conclusion

Reducing improper payments and fighting fraud within government transactions have been long-standing bipartisan priorities. Leveraging technology and data to modernize fraud prevention is essential. This paper has highlighted the benefits of data sharing in enhancing program integrity and fraud prevention. Expanding data access plays a key role in improving data quality, strengthening fraud detection, supporting evidence-based policy making, and enhancing service delivery. As agencies increasingly rely on data-driven decision making, a central challenge is the inherent tension between privacy protections and the need for data accessibility. Privacy laws and regulations protect sensitive personal data, prevent potential abuses, and ensure ethical and legal standards in government data management. At the same time, these laws introduce challenges that can hinder effective collaboration and information exchange for legitimate purposes and make it more difficult for agencies to coordinate services, evaluate program performance, or detect fraud.

While there is a consensus among stakeholders on the value of data sharing and a data-driven fraud prevention approach, it is critical to ensure that data sharing complies with privacy laws and regulations. Data must be collected, stored, and shared lawfully and in a transparent manner. The government has the responsibility to balance the individual privacy rights of citizens and the legitimate interests of government agencies.

The Study Team has recommended some legislative, policy, and structural changes along with best practice guidance to strengthen data-sharing initiatives and promote a data-driven fraud prevention approach while protecting privacy. Opportunities exist to streamline and expedite the compliance processes required by privacy laws and reduce barriers to sharing data across federal agencies. In addition, the Study Team's research highlights the need for flexibility to respond to situations where privacy laws hinder agencies' ability to access data to investigate, detect, and prevent scams and fraud. In such instances, requiring strict compliance with statutory requirements may not be practical or desirable. Special authorities or statutory exemptions would facilitate data sharing between agencies to strengthen program integrity and fraud prevention. Furthermore, more systematic reform is required to overcome cultural and structural barriers and accelerate data sharing across government agencies. Establishing a centralized data platform would strengthen agencies' ability to leverage data and data analytics to support improper payments and fraud mitigation efforts.

Further research is needed to support the implementation of these recommendations. For example, there are different options for establishing a centralized data platform to support program integrity and anti-fraud efforts, such as enhancing existing data-sharing initiatives, creating a new office within the federal government to develop and manage the data platform, or leveraging public-private partnerships. A comprehensive analysis of the strengths and limitations of each option is needed. This includes examining the technological infrastructure required to support secure data sharing, the legal and regulatory frameworks necessary to facilitate cross-agency collaboration, sustainable funding sources, opportunities to leverage states and private sector data, and the best practices for ensuring data quality, privacy, and security. The need for these measures is increasing as more government data migrates to digital form and data management technologies advance.

To implement change, Congress and federal agencies, especially leadership, must acknowledge the challenges facing data sharing and confront the barriers that have prevented actions in the past. The goal is to enable effective data sharing to enhance fraud prevention without undermining public trust or compromising privacy.

Appendix A: List of Interviewees

- **Bagdoyan, Seto**, Director of Forensic Audits, GAO
- **Banner Rone, Jenny,** Former Deputy Inspector General, USDA; Former Executive Director, Pandemic Response Accountability Committee
- **Calderon, Mariana**, Assistant Director, Data Analysis, Forensic Audits and Investigative Service, GAO
- **Cutshall, Charles,** Adjunct Associate Professor, American University
- **Dalboe, Kirsten**, Council Chair, Federal CDO Council; Chief Data Officer, Federal Energy Regulatory Commission
- **Edwards Holmes, Amy,** Partner & Principal, Holmes Consulting Group Inc.
- **Evermore, Michelle,** Senior Fellow, National Academy of Social Insurance
- **Forman, Mark,** Chief Strategy Officer, Amida Technology Solutions
- **Ginsberg, Wendy**, Director, Congressional Affairs, National Archives
- **Hendler, Jim,** Tetherless World Senior Constellation Professor of Computer, Web and Cognitive Science and Director of the Future of Computing Institute, Rensselaer Polytechnic Institute
- **Kamara, Jennifer**, Professional Staff Member, Committee on Oversight and Accountability
- **Kingsberry, Shawn,** Vice President in the Digital Innovation Factory, SAIC
- **Leder-Luis, Jetson,** Assistant Professor, Boston University
- **Lewis, Barbara,** Assistant General Council, GAO
- **Miskell, Renata,** Deputy Assistant Secretary for Accounting Policy and Financial Transparency, Office of the Fiscal Assistant Secretary, U.S. Department of the Treasury
- **O'Hara, Amy,** Research Professor, Director, Federal Statistical Research Data Center, Georgetown University
- **Paul, Kshemendra**, Assistant Inspector General for Cyber Assessments and Data Analytics, DOE OIG
- **Peaston, Sandra,** Director of Research and Development, Cifas
- **Roat, Maria**, Former Deputy Federal CIO, OMB; Academy Fellow
- **Sima-Eichler, Peter**, Assistant Inspector General for Analytics and Innovation, USDA OIG
- **Simonetta, Suzanne,** Director, Division of Performance Management, Office of Unemployment Insurance, Employment and Training Administration, U.S. Department of Labor
- **Stettner, Andrew,** Director of Economy and Jobs, The Century Foundation

Appendix B: List of Roundtable Participants

Roundtable One (1/21/25)

- **Chenok, Dan,** Executive Director, IBM Center for the Business of Government
- **Luna-Reyes, Luis,** Professor of Public Administration, University of Albany
- **Mader, Dave,** Civilian Sector Chief Strategy Officer, Deloitte
- **Reeder, Frank**, Founding Chair, Center for Internet Security
- **Wiseman, Jane,** Founder and CEO, Institute for Excellence in Government

Roundtable Two (1/30/25)

- **Cantrell, Gary,** Specialist Leader, Deloitte; former Deputy IG for Investigations, HHS OIG
- **Criscitello, Doug,** Program Integrity Fellow, Arnold Ventures
- **Cutshall, Charles,** Adjunct Associate Professor, American University
- **Calderon, Mariana,** Assistant Director, Data Analysis, Forensic Audits and Investigative Service, GAO

National Academy of
Public Administration®

1600 K Street, NW
Suite 400
Washington, DC 20006

Phone: (202) 347-3190
Website: www.napawash.org