Best Practices and Laws Governing Cross-Agency Education and Workforce Data Sharing

May 2025

Cross-agency data sharing occurs when separate agencies share data for a specific purpose. That purpose should ultimately benefit data providers and should be driven by publicly agreed upon priorities for data use. A cross-agency data governance structure that includes high-level decisionmakers from various agencies as well as public stakeholders is the most successful way to ensure that data is shared in an appropriate, transparent manner. It is also the best way to ensure an individual's privacy is protected and data is properly secured.

Why Should Leaders Share Data Across Agencies?

Cross-agency data sharing allows states to ease transitions along individuals' education and workforce pathways. For instance, it enables:

- Individuals to access streamlined admission to college or workforce training programs, benefits like SNAP for low-income families, and career pathway tools that allow students to explore the education and training needed for specific jobs;
- Policymakers and students to better understand the quality and return on investment of education programs; and
- Mayors to align their workforce investments with labor market trends and for employers to situate new businesses where there is a skilled workforce.

Critically, data sharing provides a benefit back to the people who have contributed their data. Individuals give the government information, particularly their most sensitive data (e.g., income), because it is necessary in order to receive something of value (e.g., better programs, more information) or because the government tells them they must provide it (e.g., tax information). In either case, the government agrees that, with limited narrow exceptions, it will not use the data for anything other than the purpose for which it was provided. This social contract creates the trust necessary to promote data sharing for appropriate data uses.

Data sharing by government agencies outside the bounds of established law, policy, and practice can be risky and lead to misuse. **In short, when there is no transparency or public accountability around data-sharing efforts, everyone—Congress, state and local leaders, and the public—must ask hard questions to agency leaders about what is occurring.**

Principles of Good Data Use

Appropriate and effective data uses help, not harm, people. Data must be used in a manner that abides by these long standing principles:

- **Follow federal privacy laws as well as established procedures and protocols.** Data is collected from individuals, institutions, states, and local governments for specific purposes. Each federal data collection is detailed in a

federal law or regulation that is debated publicly and either passed by Congress or enacted through public notice and comment. Numerous existing laws (like those described below) expressly prohibit the government from creating a database of individuals' information and from using data for a purpose other than that for which it was collected. Further, the usual process for cross-agency data sharing at the federal level involves, among other things, data-sharing agreements or memorandums of understanding, computer matching agreements, Federal Register notices about what data is being shared and for what purposes, and the involvement by the inspector general's office within the agency to ensure data is shared securely and in accordance with existing laws.

- **Be transparent and build trust.** Collecting and using a person's data is an exercise in trust. Working on federal data efforts in the dark is creating public mistrust of data, data collections, and data sharing. States may be hesitant about moving forward with efforts like streamlined postsecondary admissions or creating centralized processes for public benefits eligibility because they are concerned about holding too much private data for vulnerable individuals—and that the federal government might request the data for purposes not authorized by Congress.
- **Do no harm.** Individuals provide detailed, personal data to government agencies because they are either receiving a benefit (e.g., student financial aid, health care, public support through programs like SNAP and TANF) or required (e.g., taxes). In exchange for their information, they expect government officials to use that information to better the programs and services they are providing. Implicit in bargain is that the government will keep their information private and use it to benefit, not harm, them. Linking any individual-level, personally identifiable data across agencies without specific authority, public transparency and shared governance for its privacy and use, would violate this fundamental tenet of data collection.

Data is crucial to the evidence-based decisionmaking that all leaders should practice to ensure that policies and programs benefit people. But linking and sharing data behind closed doors could compromise every American's privacy and leave people uncomfortably in the dark.

Privacy Act

The Privacy Act is the primary federal statute that ensures the fundamental bargain between individuals and the government is maintained where data sharing is involved. **The Privacy Act generally prohibits federal agencies from disclosing personal information without consent except in a set of specific circumstances**. Those exceptions relate to criminal investigations, routine agency use, Government Accountability Office inquiries, statistical research, and health and safety. It's unclear that any exception would allow the sharing of data to identify "waste, fraud, and abuse," let alone for no identified purpose.

Education and Workforce Statutes

In addition to the Privacy Act, which addresses the sharing of data by federal agencies, various education and workforce statutes prohibit the creation of a national database from the data they require to be collected. For example:

- **Education Sciences Reform Act**: **"**Nothing in this subchapter may be construed to authorize the establishment of a nationwide database of individually identifiable information on individuals involved in studies or other collections of data under this subchapter." 20 U.S.C. § 9572.
- **Every Student Succeeds Act**: "Nothing in this Act . . . shall be construed to authorize the development of a nationwide database of personally identifiable information on individuals involved in studies or other collections of data under this Act." 20 U.S.C. § 7911.

- **Higher Education Act**: "Except as described in subsection (b), nothing in this Act shall be construed to authorize the development, implementation, or maintenance of a Federal database of personally identifiable information on individuals receiving assistance under this Act, attending institutions receiving assistance under this Act, or otherwise involved in any studies or other collections of data under this Act, including a student unit record system, an education bar code system, or any other system that tracks individual students over time." 20 U.S.C. § 1015c.
- **Individuals with Disabilities Education Act**: **"**Nothing in this title shall be construed to authorize the development of a nationwide database of personally identifiable information on individuals involved in studies or other collections of data under this part." 20 U.S.C. § 1416 (b)(2)(B)(ii).
- **Strengthening Career and Technical Education for the 21st Century Act (Perkins V)**: "Nothing in this Act shall be construed to permit the development of a national database of personally identifiable information on individuals receiving services under this Act." 20 U.S.C. § 2304.
- **Workforce Innovation and Opportunity Act**: **"**Nothing in this Act (including the amendments made by this Act) shall be construed to permit the development of a national database of personally identifiable information on individuals receiving services under title I or under the amendments made by title IV." 29 U.S.C. § 3341.

Other Statutes

Beyond the education and workforce realm, there are general federal statutes that govern things like Census data and federal tax information that also prohibit sharing personally identifiable data:

- According to the Census bureau, "Private information is never published. It is against the law to disclose or publish any private information that identifies an individual or business including names, addresses (including GPS coordinates), Social Security Numbers, and telephone numbers."
- Internal Revenue Code § 6103 states that "returns and return information shall be confidential" and that no officer or employee "shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section." The consequences associated with recent changes to federal student aid law, which now classify the income provisions of the FAFSA as federal tax information, bear this out. As a result even institutions of higher education have been unable to access data they previously received related to students' aid because it is now considered federal tax information governed by this provision of the Internal Revenue Code.