Know Your State's Rights to Defend Data

Stop. Think. Act: Creating Standardized Processes for Responding to Data Requests By Sarah Forland

Protect State Data to Preserve Public Trust

When we engage with public programs, register to vote, seek healthcare, and apply for benefits, we trust government agencies to adequately protect our data and only use it for the purposes for which it was shared. Government agencies at all levels are responsible for safeguarding the personal, sensitive data they hold—preventing misuse that exposes individuals to risks or undermines public safety.

However, recent actions by the U.S. federal government are pressuring states to open their data systems in ways that depart from long-standing and ethical norms. These actions may even violate state or federal laws and rules, as the administrative data gets used outside of its intended purpose. **It's more important than ever for states to stand up for their residents' privacy and safety and take action to better manage and protect state-held data.**

Preparing for and Responding to Data Requests

Whether a request comes from the federal government, third-party vendors, or law enforcement, granting any data access without rigorous, systematic review can erode the very systems states rely on to effectively serve residents. Chief data officers (CDOs), chief privacy officers (CPOs) and chief information officers (CIOs) should collaboratively develop and standardize a process for state agencies to evaluate and approve or deny any data sharing request; whether it be inter- or intra-agency, from a third-party vendor, or from a federal agency. ***Creating a standardized process can help state agencies prepare for and respond to inappropriate requests for data.*** This process should accomplish the following:

- Provide relevant legal and policy guidance on required data sharing and protections: In consultation with a state's Attorney General's office, state data managers should create and use a resource to help state agencies assess the legality of data sharing requests. This resource should include any relevant federal and state law, programmatic specific laws or requirements, as well as the state's own data privacy and security policies.

- Designate and identify individuals and offices that can assist state agencies in responding to requests: A standardized process for evaluating data sharing requests should designate and identify (1) individuals or offices within each state agency responsible for evaluating requests; (2) individuals or offices that can help states assess the legality of requests; and (3) individuals or offices that state agencies should provide notice of approved requests for oversight and transparency.

- Design a rubric to evaluate requests: A rubric for state agencies to assess data sharing requests should evaluate (1) the legality of the request; (2) the necessity and scope of the request, to ensure the requested data is pertinent to the stated goal and maintain data minimization practices; (3) the privacy impact of granting the request; (4) privacy and security practices of the entity requesting access to the data.

- Assign clear data privacy and security requirements to approved requests: If a data access or sharing request is approved, any memorandum of understanding (MOU) or data sharing agreement (DSA) should clearly outline data privacy and security requirements. This guidance should take into account what data is being shared, the purpose of data sharing, and the duration of access. Wherever possible, technical safeguards should be implemented to ensure that data cannot be accessed outside the stated purposes and timeline of the MOU or DSA.

- Create a notice scheme to report approved requests and flag inappropriate requests: In consultation with a state's Attorney General's office, state data managers should develop a notice scheme to report approved data sharing requests and to flag any data sharing requests deemed inappropriate or unlawful. Notice should be provided to all relevant parties, as identified by state data managers and the Attorney General's office, in a timely manner to improve transparency and oversight. In addition, processes should be in place to identify and correct/terminate any mistakenly granted data requests.

- Create a response system for legal actions related to data requests: State data managers should work with relevant legal departments and the state's Attorney General's office to identify a response system for any legal actions related to data requests—such as requests stemming from judicial or administrative warrants, subpoenas, or court orders. This response system should inform agencies how to appropriately respond, flag, and disclose such legal actions.

Contact Us

Sarah Forland
Policy Analyst
forland@newamerica.org

Sydney Saubestre
Senior Policy Analyst
saubestre@newamerica.org