

Stop. Think. Act.

5 Questions to Answer Before Responding to a Request for State Data

Since January 2025, the federal government has made unprecedented efforts to inappropriately access the personal data of hundreds of millions of U.S. residents. As a result, state databases and federal agencies have become a target of federal overreach – as seen in the demands for state voter data, SNAP recipient data, and Medicaid recipient data.

To facilitate public services and benefits, states collect and hold a wide range of personal data about residents. This information is protected by various state and federal rules and regulations, which require privacy protections and limit the legal use of collected data.

As trusted stewards of the public's personal information, state agencies are the front-line defenders against such data misuse. States can earn and keep the public's trust by asking the right questions when data is demanded.

Is this legal?

1

Assess the legality of a data access request.

Laws at the state, federal, or programmatic level require data privacy and security measures and limit using collected data to specific purposes. State agencies should develop a clear process to determine the legality and compliance requirements of data requests.

Is this necessary?

2

Determine if and what data is needed to meet stated tasks of a data use or share request.

Requests to access or share data should have a clear, limited purpose, and **access to identifiable data should only be granted if absolutely necessary**. Data should not be shared or used for any reason outside of the purposes for which it was collected or generated.

What's the impact?

3

Evaluate the potential impact of sharing personal data. **Sharing data outside its intended purpose can introduce privacy and security vulnerabilities**, enable misuse that puts individuals at risk, and weaken public trust. To evaluate the potential impact, states can conduct privacy impact assessments, examine the privacy and security practices of the requesting party, and analyze the potential for misuse.

Who should know?

4

Maintain a clear system for providing notice of data-sharing requests.

Protocols should identify individuals or offices that evaluate a data sharing request as well as those that require timely notice of whether a request is granted or flagged as potentially inappropriate or unlawful. By providing greater transparency and oversight of data use, such protocols create an avenue to identify and correct or terminate any mistakenly granted requests.

Who can help?

5

Identify and consult expertise throughout the state when responding to requests. **States agencies shouldn't navigate high-risk data decisions alone**. Legal experts, data management officers or technical consultants, or other state agencies managing parts of the requested data set can provide input and guidance to ensure data protections are upheld and prevent inappropriate disclosure of state held data.