B.2: Talking Points — Setting reasonable privacy expectations

Many stakeholders will not appreciate what is—or is not—realistically possible to do with integrated data, and so may overestimate the risks to individual privacy and civil liberties. Similar confusion often exists about the efficacy and applicability of various privacy safeguards, which can make it difficult for stakeholders to evaluate actual privacy risks and data benefits. It is important to build trust by communicating specifically how data will (and will not) be used and how it will be safeguarded.

Key strategies and messages:

- **Communicate the realistic capabilities and limitations of integrated data.**
  - The analysis of integrated data provides agencies with valuable information about what we are doing well and where we need to make improvements.
  - Although administrative data may include personally identifiable information, the IDS cannot single out or target individuals for action of any kind. We are forbidden by law from doing so and have stringent safeguards and accountability measures in place, such as _____. (See Appendix A.1 for examples).
  - An IDS is only as good as the data it integrates. Before we link data across domains, we work with the agencies that collect it to identify which elements are high quality and relevant to the questions at hand.
  - Even aggregated data (where no personal information is included) about patterns of service use can help our government make decisions about _____ and _____.
  - Integrated data is key to evaluating our current policies, but that is just step one in evidence-based policymaking. Related policy and program changes may still take several months/years to implement.

- **Communicate the realistic capabilities and limitations of your privacy program.**
  - Our IDS has a comprehensive privacy and security policy that clearly outlines the controls and safeguards in place to protect administrative data. (Include any additional, specific safeguards that your IDS is relying on, e.g., only using the data necessary to achieve your goals, never sharing personal data with third parties, access controls, use limits, accountability and audit mechanisms, etc.) (See Appendix A.1 for examples).
  - Privacy and security experts were consulted at every stage of the IDS development process.
  - We comply with multiple federal and state privacy laws that protect administrative data (such as FERPA or HIPAA), and are subject to strict penalties if this data is misused or compromised.
  - Although there are no “silver bullet” solutions to privacy problems, our IDS employs a variety of technical, procedural, legal, and organizational safeguards to significantly reduce privacy risks.
  - We have done our best to anticipate how integrated data will impact our communities, but it is not always possible to eliminate all privacy and security risks. We have several open channels for concerned community members or other stakeholders to raise concerns, complaints, or vulnerabilities, including [link or contact information].
  - Privacy and security management and data protection are on-going systems that are continuously monitored, updated, and supported by trained personnel to ensure they meet the highest standard over time, not just at initial implementation.

- **Articulate the benefits and risks of innovative data use.**
  - Our IDS seeks to maximize data’s benefits to the community, such as using data to ensure tax dollars are used efficiently and that our public services are being distributed equitably and effectively within our community—while minimizing risks.
  - We have carefully assessed both the potential benefits and privacy risks of this use case and believe that the substantial benefits to our community outweigh the minor risks. Specifically, our analysis showed _____. (See Data Benefit Analysis exercise below).

› **Differentiate between the IDS' legal, ethical, and equity-based obligations.**

- Our IDS goes above and beyond basic legal compliance to protect your privacy.
- We are committed to only using integrated data in ways that are ethical and equitable to everyone in our community.
- Our choices about data and privacy are informed by legal, ethical, and policy guidelines relevant to our community, such as _____, _____, and _____. (For example, your city or state's Privacy Principles, relevant state or federal laws, or ethical codes of conduct).