

Indiana Is Investing in Human Capacity and Privacy Leadership



For states to build statewide longitudinal data systems (SLDSs) that are designed to ensure that people have access to the data they need, state leaders must consider the human capacity they already have, and must develop, to support this work. Building the human capacity required to manage, analyze, and protect data means investing in and developing a skilled workforce that is capable of not only handling large volumes of data but also making sure that the data is relevant, accurate, and accessible to those who need it—including individuals planning their career paths, educators making decisions to support students, or policymakers shaping public policy. To achieve this goal, states should create clear career pathways for data professionals, offer continuous professional development, and foster expertise in both data analysis and data privacy.

Indiana's approach demonstrates the impact of investments in data workforce and privacy capacity and can serve as a model for other states. These efforts can lead to more effective and innovative data use and also ensure compliance with legal and privacy requirements. By prioritizing human capacity, states can maximize the impact and utility of their data systems, which ultimately empower individuals, educators, and policymakers with the information they need to make informed decisions.

Developing Career Pathways for Data Professionals

A well-trained workforce is essential for managing and protecting data in ways that support decisionmaking and compliance with privacy regulations. However, without clear career pathways and hiring structures for data professionals, states can struggle to maintain the workforce they need. By developing these pathways and hiring structures, states can build and retain the expertise they need to ensure that state data systems are accessible and effectively used by the policymakers, educators, and families who rely on them. Investing in these efforts not only enhances data system usability and sustainability but also helps attract and retain skilled professionals in the public sector, ensuring that states can answer critical policy questions and drive better outcomes.



Indiana has addressed this challenge by modernizing career ladders for data and evidence staff, updating job classifications, and creating structured pathways for professional growth. To accomplish this, a working group representing 20 state agencies, led by the [Indiana Data Governance Council](#), revised and created job descriptions and eliminated outdated classifications. Initially focused on specific roles to fill smaller workforce gaps, this effort expanded into structured career ladders with clearly defined levels—associate, intermediate, senior, and supervisor. Along with these updated descriptions and specifications, Indiana is developing hiring roadmaps for small, medium, and large data teams across different state agencies, ensuring that they build workforce capacity in a way that meets both current and future needs. These updates promote consistency in hiring

and career progression across multiple state agencies, including Indiana’s Management Performance Hub, which oversees the state’s SLDS. Indiana also supports professional development by offering training and certification programs for data officials along their career journeys.

To further strengthen career pathways and early entry into the field, Indiana partners with Purdue University’s Data Mine program. Currently in its pilot phase, the program provides students with hands-on learning opportunities through real-world projects and co-op-style experiences. This partnership helps build a pipeline of future data professionals while equipping them with practical skills for public-sector roles.

Embedding Privacy Leadership Across State Agencies

As states collect, analyze, and share data across agencies, centering privacy is crucial. Indiana has taken a structured approach to privacy governance by embedding agency privacy officers (APOs) across all state agencies to ensure compliance with privacy laws and proactively manage data protection concerns.

A well-developed privacy and data protection workforce strengthens compliance, builds trust among stakeholders, and enhances the efficiency of state agencies by ensuring clear and consistent management of sensitive information.

Indiana has assigned privacy officers across numerous business units in state agencies, including the executive branch, courts, and Legislative Services Agency. The role of [APO](#) follows a clearly defined, consistent job description statewide, with responsibilities focused on:

- ensuring compliance with state and federal privacy laws;
- managing privacy risks; and
- collaborating closely with the state’s chief privacy officer on matters such as artificial intelligence (AI) implementation and data sharing.

Privacy officers were selected based on their existing expertise, roles in data governance or regulation, and familiarity with their agency’s data practices. They receive standardized training designed to build consistent knowledge and practices across all agencies.

Indiana’s privacy officer initiative faced challenges, including high demand for training opportunities and concerns about balancing new responsibilities alongside existing roles. To address these issues, Indiana is providing additional training sessions, establishing regular office hours for privacy officers to network and exchange best practices, and developing a dedicated online resource repository. Additionally, privacy officers actively participate in policy discussions on emerging technologies, including AI and data sharing, and have helped introduce standardized templates for data-sharing agreements. Through these efforts, Indiana reinforces privacy protections as a foundational aspect of evolving data governance practices across the state.

How Federal Support Can Help

Enhancing federal and state collaboration is essential to supporting initiatives like Indiana’s and helping other states build similar programs. The federal government continues to have a role to play in supporting states in this work, and doing so requires staff and support—

both technical assistance and resources. **Establishing a more uniform federal privacy law** would help simplify compliance, reducing the burden of navigating varying state and sector-specific regulations. The federal government could also play a direct role in supporting

initiatives like Indiana's privacy officer program by **offering targeted grants, training resources, and standardized privacy frameworks** for states to adopt. Finally, federal support could help to improve the development and sustainability of state data workforces through **unified grant guidance and consistent language from the US Department of Education and the US Department of Labor on demographic data**

collection and use. Indiana has faced challenges with differing interpretations of grant requirements and data use conditions, leading to inconsistencies in data collection and application of policies. By addressing these challenges, federal agencies can help states focus more on improving data privacy and workforce capacity, rather than managing inconsistencies in requirements and funding conditions.

Lessons From Indiana's Approach

Indiana's approach demonstrates how states can strengthen human capacity and enhance privacy protections within their data systems. Key lessons from Indiana's approach include:

- **Invest in structured career pathways and talent pipelines** by modernizing job classifications, clearly defining career ladders, and partnering with universities or local organizations to create sustainable workforce solutions. Indiana's approach of aligning career pathways with agency needs and leveraging partnerships with institutions like Purdue University helps attract and retain skilled data professionals while reducing turnover and ensuring long-term capacity.
- **Embed privacy and data governance expertise across agencies** by integrating dedicated privacy officers within agencies to enhance compliance, strengthen risk management, and ensure that privacy considerations are seamlessly incorporated into daily operations. Indiana's model demonstrates how structured deployment of privacy officers fosters shared responsibility and alignment with workforce strategies.

- **Sustain workforce and privacy investments through long-term cross-agency collaboration and leadership support** by ensuring strong coordination across departments, dedicated funding, and long-term leadership commitment. Institutionalizing career pathways, privacy roles, and professional development efforts helps to ensure that these investments remain integral to state data systems rather than temporary solutions that fade with leadership or funding shifts.

Indiana's approach to workforce capacity and privacy leadership highlights the impact of investing in people to ensure that data systems are effective, secure, and sustainable. By modernizing career pathways, embedding privacy leadership, and fostering cross-agency collaboration, the state has created a roadmap for others. As states advance data modernization efforts, they can follow Indiana's lead by prioritizing workforce investments and privacy leadership to create sustainable, people-centered systems.