Transforming How
Texas Government
Serves Texans

Data Sharing Best Practices

Data Management Advisory Committee

Office of the Chief Data Officer
Texas Department of Information Resources

July 2023

Table of Contents

Introduction

Data sharing helps maximize data as a valuable organizational asset, and its importance cannot be overstated. The benefits of data sharing are many but ultimately include improved decision-making to advance an organization's mission and goals, increased transparency and accountability, cost savings, and increased constituent trust.

Many Texans receive services provided by multiple state-sponsored programs. Sharing data across government organizations and departments provides a more comprehensive view of what services are being utilized by what people and therefore has the potential to transform how policies are made and how services are delivered.

For example, the COVID-19 pandemic disrupted school meal services and many families lost access to free or reduced-price meals through the schools. With federal funding, the Texas Health and Human Services Commission (HHSC) issued food benefits to families affected by the loss of this service through the Pandemic Electronic Benefit Transfer (P-EBT) program. However, HHSC does not have access to all the data required to determine eligibility for the program. The Texas Department of Agriculture (TDA) has data on which schools participate in the National School Lunch Program (NSLP), and the Texas Education Agency (TEA) has data on which students are enrolled in those schools. A cooperative data sharing effort between these three agencies, combining data collected from different transactional sources, was essential for determining eligibility for the P-EBT program.

Sharing data among relevant stakeholders can also enhance fraud, waste, and abuse detection and prevention efforts by pooling information to identify patterns and anomalies not possible by analyzing one organization's data alone. For example, a data sharing effort between the Texas Natural Resources Information System (TNRIS) and the Texas Department of Insurance (TDI) allowed TDI fraud inspectors to use TNRIS data on storm tracking and potential damage locations. By incorporating TNRIS data into their analyses, TDI fraud inspectors were able to respond quickly and accurately to prevent post-storm insurance-based fraud activity.

Publishing on the Texas Open Data Portal (ODP), the state's central repository for public data, can significantly benefit public agencies' ability to fulfill data-sharing requests efficiently and effectively. Utilizing the ODP, agencies can streamline responses to requests made under the Texas Public Information Act and reduce the need for multiple, separate requests to different agencies. Time and resources are conserved for both the requesting party and the agencies, as the Open Data Portal provides data in a self-serve format that can be tailored to individual needs. The platform also provides a secure and consistent method for sharing data, reducing the risk of data breaches, and allowing all data users access to the same information.

Sharing data across organizations and departments can increase efficiency and reduce costs by eliminating duplicative data collection activities. Data can be accessed quickly through automated transfer processes and data users can be confident in the consistency of data analyzed within and across different teams.

Good data governance and efficient data management is vital for data sharing both within an organization and with external partners, including other organizations or the public. Data Management Officers (DMOs) and others within the organization who work with data must understand the impact of these principles on successful data sharing, as well as the potential challenges that might impede data sharing activities, and how to work with others to overcome those challenges.

Challenges

There are many challenges and obstacles that can hinder an organization's ability to effectively share and use data. Some of the more common challenges are described below.

- **Organizations are often unaware of data availability and sharing authority.** Data and information are created constantly. Organizations and their employees must understand what data exists under their protection and what their responsibilities are as informed data stewards of this strategic asset. However, data users within an organization are often unaware of what data is available, what it can be used for, and what can be legally shared with others. A lack of data catalogs or inventories make it difficult to determine if an organization has the necessary data available for analytics and business intelligence, and whether certain data have legal or regulatory restrictions for sharing or use.
- **Data are often in siloed systems, are not interoperable, and have no common architecture.** Even when data sources are known, those sources often exist in siloed or isolated systems with no common architecture and file naming standards. Therefore, they are not interoperable with each other, and data sharing and use cannot proceed without labor intensive data cleansing and formatting activities. These activities often introduce risks, such as data errors and reduced data quality.
- **There is general mistrust in data sharing.** An organization may need to contend with a lack of trust in the data sharing process, which is influenced by data security and privacy concerns, and potentially conflicting goals and interests.
- **Legal processes or requirements are often unclear. What** data can be freely shared and what data is classified as sensitive, confidential, or protected according to privacy and security laws and regulations is not always clear. Further, policies and procedures detailing requirements for ensuring the appropriate legal processes are in place and followed in order to share sensitive, confidential or protected data are often lacking or not known by staff involved in potential data sharing activities. As a result, data sharing requests are often denied without a full understanding of when and how data can be appropriately shared.
- **Organizations may be unaware of available data sharing platforms.** When sharing data within or outside of an organization, there is often a question of where to store

large amounts of data where all parties in the data sharing process have access and all proper privacy and security protocols are in place.

- **Securing buy-in from leadership and stakeholders may be difficult.** Gaining approval from organizational leaders and stakeholders is often a deciding step in engaging in data sharing endeavors. Data sharing may require resources for tasks such as modifying IT infrastructure for compatibility and enhancing data quality. The advantages that data sharing provides to the organization and the public may be underestimated or unknown by leadership and stakeholders, making the allocation of time and financial resources a low priority if no clear business benefits are evident.

Best Practices

It is clear there are many challenges that can interfere with an organization's ability to share data, both internally and with other organizations. However, there are some best practices organizations can follow that may address and mitigate those challenges, allowing organizations to realize the benefits of sharing data, including improved transparency and accountability, and better provision of services.

Data Management policies and procedures

Key among these best practices is the adoption of a robust data management program to effectively manage organizational data for appropriate data sharing. As part of an overall data strategy that supports data sharing initiatives, organizations can focus on the design and implementation of comprehensive data catalogs that allow data to be discoverable and describe when and how certain data can be shared; the formulation of policies and procedures that describe how sensitive, confidential, and protected information is handled and protected; and the establishment of standards to encourage common data architectures and enable interoperability between data systems.

While there are several other data management principles that can aid in overcoming data sharing challenges, the lack of awareness of available data, understanding sharing authority, and the lack of interoperability are discussed here.

Data Catalogs

Texas state agencies and institutions of higher education rely heavily on data for making informed decisions to help them advance their organization's mission and goals. To share and use data effectively, organizations need to know what data they have at their disposal, where it is located, and who can use it and for what purpose. Data catalogs provide a way to organize information about data assets so they can be used for strategic advantage.

At a minimum, data catalogs provide a means for data users to find and understand the data managed by the organization. On the other end of the spectrum, some data catalog tools have advanced capabilities that include extensive data preparation, analysis, and visualization functions, as well as security and governance features.

Regardless of what tool is used to inventory data, or what capabilities the tool has, data catalogs provide information about data assets allowing users to find data available within the organization, choose the appropriate dataset, and view the metadata to understand where the data came from, what it means, who can access and use it, and for what approved purposes. Data catalogs can also provide indications of data quality and frequency of usage, to help users understand which data assets might be the most appropriate to use and share. Having this information readily available facilitates efficient and appropriate data sharing while protecting those data assets with sensitive, confidential, or protected information from inappropriate sharing and use.

Data Classification

Data classification is the process of organizing data into different categories based on level of sensitivity and the degree to which it needs to be protected. It helps to ensure that sensitive information is not disclosed accidentally or inappropriately, and receives protection according to the relevant laws, regulations, and organizational policies. This information is often incorporated into an organization's data catalog to make it more easily accessible to users.

Data classification enables responsible data sharing by providing clear guidelines for who can access and use which types of data and under what circumstances. It helps ensure that only authorized individuals have access to sensitive information and that it is only shared when necessary and appropriate.

The Department of Information Resources (DIR) Classification Guide and Template are available on the DIR website to assist organizations in their data classification efforts.

The successful execution of data classification activities relies heavily on effective collaboration among four essential personnel roles: Data Management Officers (DMOs), Information Security Officers (ISOs), Data Privacy Officers (DPOs), and Record Management Officers (RMOs). These key roles each contribute unique expertise to protect an organization's data.

DMOs are responsible for managing data so it remains well-maintained and accessible, and ISOs focus on providing appropriate access to data while guarding against potential breaches or other intentional misuses. DPOs provide guidance on adherence to all relevant privacy and confidentiality laws and regulations impacting data to protect the institution against undesired litigation issues related to non-compliance. Finally, RMOs manage and document data activities at the end of the data lifecycle, including the archiving and/or disposal of data, so that data that is beyond its retention schedule is not shared or used.

Standardization and Interoperability

The lack of common architectures and interoperability create major hurdles in data sharing initiatives. A report released by the Interagency Data Transparency Commission in 2016 recommended the establishment of common shared file structures and naming conventions to improve data sharing between organizations. The use of standardized, common file structures and naming conventions improves the consistency of data, and facilitates more accurate results when integrating data from different sources. For example, dates can be collected and stored in different formats or structures, and county names can be collected and stored in a variety of

naming conventions such as full names, abbreviations, or codes. In these examples, standardization policies can establish official methods of recording and storing dates and county names to promote consistency across datasets and systems.

Likewise, data cleansing standards promote consistent processes when profiling, transforming and cleaning data for analytic use. Data cleansing activities are often done on an ad hoc basis and introduce the risk of inconsistency both within and between datasets if no standards are in place. Standard processes for activities such as removing duplicate or irrelevant observations in the data, adjusting structural errors or inconsistencies, filtering unwanted outliers where appropriate, and addressing missing data, can improve the consistency and accuracy of data, as well as improve the results of analyses performed during data sharing efforts.

An organization's Data Governance Council, under the guidance of the DMO, is responsible for establishing policies and procedures related to data standardization and interoperability. Documentation of these policies and procedures describing file structures and naming conventions, and data cleansing standards and activities should be provided to all parties involved in the data sharing process to maintain data quality throughout the process.

An example of an effort to promote standardization and interoperability is the Texas Electronic State Business Daily (ESBD). The Texas Comptroller of Public Accounts (CPA) created the ESBD to be a comprehensive database of information about state government procurement, including bid opportunities and contract awards. The ESBD implemented standard file structures, naming conventions, data cleansing processes, and a golden record system to collect precise and consistent procurement data. The current iteration of the ESBD provides a vehicle for Texas agencies to submit their open market procurement opportunities for review and delegation, then advertise their procurement opportunities in a platform designed to guide them through the statutorily mandated posting steps.

By using standardized data management practices, the ESBD can improve the quality of the procurement data it collects and ease the process for state agencies sharing accurate and reliable information with vendors and stakeholders. These practices have improved decision-making, transparency, and efficiency in state government procurement processes.

Legal Processes

As state agencies and institutions of higher education continue to amass large amounts of data, adherence to complex privacy laws and regulations, security protocols, and data protection laws becomes increasingly nuanced. To enhance awareness of data sharing best practices, organizations can provide training to employees that provides insight into the laws and regulations impacting the use of data specific to the organization, and to the policies and procedures that enable legal, appropriate data sharing, both within and between organizations. Training on ethical data handling can also increase trust in the data sharing process.

Legal processes may vary from organization to organization and data users should consult with their legal counsel to gain an understanding of the requirements specific to the data within their organization. However, some baseline information on data sharing agreements and ethical data handling are described here.

Data Sharing Agreements

Organizations should enter into a contractual agreement before sharing sensitive, confidential, or protected data. Depending on the organization and type of data shared, certain laws may require specific terms for data sharing agreements, business use agreements, memorandums of understanding, or other types of legal agreements to share data. Typically, agreements will include a description of the data being shared, the purpose for sharing the data, the parameters under which the data may be used, citation of the law or regulation that provides the authority to share the data and for what purpose, and agreement by all parties that the sharing and use of the data complies with relevant privacy laws and regulations. Agreements may also include information security requirements and details about the method of transferring the data.

Organizations wishing to enter into a data sharing agreement should have policies and procedures describing the process for implementing data sharing agreements or other legal documents, requirements for compliance with privacy regulations and security measures, and a description of the roles and responsibilities of all parties involved in data sharing initiatives. Collaboration with the organization's Privacy Officer, or similar role, and regular review of privacy laws and regulations and security requirements are essential to keep abreast of new legal requirements and emerging security threats.

Texas Statewide Data Exchange Compact

To facilitate a consistent method of compliance with state and federal laws and regulations regarding data sharing and data security, the Texas Statewide Data Program established the Texas Statewide Data Exchange Compact, or TSDEC.

The TSDEC is a uniform data sharing and data security agreement for participating Texas state agencies and institutions of higher education. It contains the standard terms and conditions applicable to all agencies interested in data sharing and exchange. Once executed by all parties, the TSDEC enables a more efficient and effective process for sharing data.

The TSDEC contains two components:

- The main uniform agreement includes basic terms and conditions applicable to all data sharing agreements. By using the TSDEC, agencies can streamline the preliminary procedures and conversations between the disclosing agency' and the receiving agency.
- Participating agencies may utilize the second component, which is designed to allow the program areas to add specific statutory, regulatory or other limitations applicable to the particular data being shared by the agency.

The TSDEC may not contain all the required terms that an organization needs to allow data sharing due to program-specific laws and regulations around data. Organizations should consult with their legal counsel to determine what is required to comply with these various laws.

For more information on participating in the TSDEC, contact the Office of the Chief Data Officer at ocdo@dir.texas.gov.

Ethical Considerations

All employees of Texas state agencies and institutions of higher education are responsible and accountable for ethical data handling and preserving privacy with an appropriate level of transparency. Ethics are principles of behavior based on ideas of right and wrong, and these principles often focus on concepts such as fairness, respect, integrity, transparency, and trust. Data ethics are the norms of behavior that promote appropriate judgments and accountability when creating, managing, sharing, using, and disposing of data. While data may seem as if it is merely technical information, its use must be guided by ethical principles, or it will present a risk to an organization's success.

The Federal Data Strategy outlines seven fundamental principles for ethical data use:

1. Uphold applicable statutes, regulations, professional practices, and ethical standards.
2. Respect the public, individuals, and communities.
3. Respect privacy and confidentiality.
4. Act with honesty, integrity, and humility.
5. Hold oneself and others accountable.
6. Promote transparency.
7. Stay informed of developments in the fields of data management and data science.

Using these ethical principles as a guide, Data Management Officers can work with their organization's Privacy Officer or legal counsel, to develop policies and training to address ethical behavior regarding data specific to the organization.

Data Sharing Platforms

There are several options to address the lack of open or secure data sharing platforms.

Open Data Portal

Multiple avenues or platforms for sharing data are available to state agencies and institutions of higher education. One such platform is the Texas Open Data Portal (ODP), hosted by the Texas Department of Information Resources (DIR).

In 2019, Senate Bill 819 of the 86th Texas Legislature, Regular Session, established the ODP as the official central repository for publicly accessible electronic data. In 2021, Senate Bill 475 of the 87th Texas Legislature, Regular Session, directed agencies with a minimum of 150 full-time employees to post at least three high-value data sets on the ODP, marking the beginning of an effort to consolidate and enhance data sharing for State of Texas open data.

Open data refers to information that can be used, reused, and redistributed by anyone. It is made accessible in a format that is easily consumed and can be read, filtered, sorted, manipulated, and combined with other data. Open data found on the ODP is available at no cost and viewed and analyzed directly on the platform or downloaded for offline analysis.

As data published on the ODP is intended for public consumption, only publicly accessible data should be made available. Note that protected, sensitive, and confidential data should never be published on the ODP.

The ODP has tremendous potential for governmental entities to redirect a public information request to data that is already publicly available. This offers a great economic benefit to governmental entities and the public, as it reduces the number of public information requests, decreases overhead associated with handling the requests, and generally improves the data user experience for accessing open data of all varieties.

The ODP can be found at data.texas.gov. Additionally, the Texas Data Portals Resource Guide provides information on how to get started with publishing and sharing data, as well as suggested governance policies and procedures organizations can adopt.

Closed Data Portal

Not all data is open data, however, and an organization may need to share sensitive, confidential, or protected data.

The Closed Data Portal (CDP), also hosted by DIR, is a private data sharing platform for sensitive, confidential, or protected data. It uses vertical data sharing between departments within the same organization or horizontal data sharing between multiple organizations. The CDP is able to host data containing Personally Identifiable Information (PII)*, and access to a CDP instance is by invitation only. Unlike the ODP that is administered by DIR, the sponsoring organization of the CDP instance manages all data, content, and settings, including: viewing audit trails, configuring site appearance, creating and managing users, roles, and permissions, and creating a site-wide metadata schema. A best practice is to have at least two administrators from the sponsoring organization to facilitate adequate oversight of the CDP.

*TX-RAMP Eligibility and Requirements | Texas Department of Information Resources

Cloud Technologies

The Open and Closed Data Portals offer efficient and secure data sharing through the use of cloud platform technologies. Cloud platforms make use of computing resources available over the internet to provide access to data without requiring internal, or on-prem, storage systems.

Cloud-based platforms are available in public, private, and hybrid options with robust security measures, and they promote cooperation between departments with regulated access permissions to facilitate sharing of relevant information. Platforms are scalable to handle large amounts of data and have backup strategies and disaster recovery approaches to protect against loss.

The DIR Texas Data Center Services program allows state and local governmental agencies to outsource management of technology infrastructure services and provides secure connectivity to select public and private clouds. More information can be found on the DIR Texas Data Center Services website, or consult with your Chief Technology Office to find out what cloud-based platforms might be appropriate and available to your organization.

Considerations for Data Quality & Security Controls

When implementing any data sharing platform, organizations must establish data quality standards to provide assurance the data is timely, accurate, accessible, and appropriate to the intended audience. Data sharing platforms are usually managed and maintained by a number of data stewards spread throughout an organization; consequently, security controls must also limit publishing roles and actively screen for noncompliant or unauthorized publishing. Agencies and organizations should consider the following data sharing practices as success criteria for data quality and security:

- **Foundation in Policy & Process**: Publishing to the data sharing platform is requested and tracked through a standard business process for configuring and posting the data, and centralized through a lead administrative team for the organization, which assigns editing and publishing roles on the principle of least privilege: granting minimal access strictly for the right users to perform limited job functions. As part of the standard process, detailed information on the data's business case, ownership, metadata, and data sourcing are uniformly captured and stored in a data catalog. Administrators for the data platform will review all requested data for noncompliance (e.g., sensitive personal information in public data), advise on data formatting and presentation to ensure data is optimized and accessible for intended audiences, and educate publishers on standards for long-term data maintenance and stewardship.
- **Preventative Measures**: Administrators for the data sharing platform will conduct standard periodic reviews for data quality and compliance, in context of data privacy laws and regulations, as well as the organization's policies and standard operating procedures. Data quality is assessed through measurable qualifications, such as pass/fail criteria and quantifiable benchmarks, which are used to coach data stewards and resolve data quality and security issues. Where possible, secure automation methods are developed for scheduled dataset updates, to promote the currency and accuracy of the data and the efficiency of dataset management.
- **Tools for Informed Response**: Notifications and distribution systems are in place to monitor for and respond to stakeholder inquiries, automation failures, and the unauthorized publishing of data, where mitigation strategies and response plans are established to address these scenarios. Data analytics (e.g., site metrics which track customer impact and website referrals) are frequently utilized to inform leadership on the usage of shared data and promote organizational alignment on enhancing the availability and presentation of the data.

Data Management Officers should work with their organization's Information Security and Privacy Officers, as well as the Records Management Officer, to develop standards and controls to govern the appropriate use of data sharing platforms. By creating policies to define standards and controls as the foundation of data sharing procedures, and providing training to help reinforce these concepts, organizations can maximize the benefit of their data sharing platform and minimize, or eliminate, associated security risks.

Change Management

Securing leadership buy-in for data sharing initiatives starts with having clearly defined goals and objectives for those initiatives. Not only are goals and objectives essential for gaining buy-in from leadership and stakeholders, they keep everyone aligned on what is to be achieved. However, securing buy-in often requires change management – a process that provides a structured approach to communicate the benefits of sharing data, address potential concerns and resistance to change, and ensure that the necessary resources and processes are in place to support the initiative.

Various strategies exist for implementing change management effectively. Public agencies can adopt frameworks like the research-action technique based on the Burke and Litwin model or Lewin's three-stage model to design a robust change management approach. Resources and frameworks provided by the American Society for Quality can also be integrated into organizational processes to secure the necessary buy-in for data sharing initiatives.

Effective communication and a persuasive argument for data sharing are essential in garnering support from leadership and stakeholders. Employing a systematic change management strategy allows public agencies to present a practical, evidence-based approach to enact organizational change, encompassing changes associated with data sharing and data management. Consequently, public agencies can successfully navigate the intricacies of organizational transformation and enhance their data sharing efforts and initiatives.

Data Literacy

Effective communication with business leaders and stakeholders is necessary in promoting data sharing activities. Communicating the value of data sharing requires improving and enhancing data literacy among all data users within the organization. Showcasing scenarios where data sharing is a critical and measurable factor of success can help build support and increase buy-in from critical decision makers. Defining success can demonstrate the value of data sharing and encourage wider adoption and can build trust and foster a culture of data sharing within the organization.

Communication is a two-way street, so it is imperative that everyone who uses data, including leadership and stakeholders, speaks about data in a consistent, common language. Improving and enhancing data literacy involves training all data users in several key areas.

- **Understanding data:** Knowing what is meant by "data" and how it impacts business decisions and outcomes.
- **Finding and Obtaining data:** The awareness of available data sources and which sources are most relevant to answer particular questions.
- **Reading data:** The ability to interpret data presented in multiple formats and the ability to evaluate data and results critically, rather than taking them at face value.
- **Managing data:** Awareness of data management principles, including data quality, master data and metadata management, records management, and privacy and security.

- **Using data:** The ability to prepare data for analysis, analyze data appropriately, and use the necessary tools, as well as understanding the ethical use of data.
- **Communicating with data:** Understanding how to use data to support a larger narrative that is intended to communicate a message or story to a particular audience.

Increasing and enhancing data literacy among all data users in the organization, including business and program leadership, will go a long way in addressing the challenges described in this white paper. DMOs can help increase data literacy within their organizations by participating in the DIR Texas Data Literacy Program and by developing their own organization-specific data literacy programs.

Conclusion

Data sharing is a powerful tool for Texas state agencies and institutions of higher education to improve decision-making, service delivery, and transparency. However, challenges and obstacles such as data silos and interoperability, lack of trust, legal and security concerns, and securing buy-in from leadership and stakeholders can impede data sharing efforts. To overcome these challenges, organizations can adopt best practices such as implementing data management policies and procedures to support data sharing, improving data classification, and standardizing data to support interoperability.

Additionally, organizations must follow legal processes and practice ethical data handling to maintain privacy and confidentiality, protect civil liberties, and maximize the public good. Cloud-based platforms can facilitate the secure and governed sharing of data, and addressing change management and data literacy in the organization can help secure buy-in from leadership and stakeholders. By implementing these best practices, public agencies can improve decision-making and provision of services, enhance the detection and prevention of fraud, waste, and abuse, and increase transparency and efficiency, leading to better outcomes for the organization and the public.

References

Texas Open Data Portal | Texas Department of Information Resources
https://dir.texas.gov/office-chief-data-officer/texas-open-data-portal

Data Governance and Data Catalogs: Where Do They Intersect? - DATAVERSITY
https://www.dataversity.net/data-governance-and-data-catalogs-where-do-they-intersect/

DIR Data Classification Guide
https://dir.texas.gov/resource-library-item/data-classification-guide-v11

DIR Data Classification Template
https://dir.texas.gov/resource-library-item/data-classification-template

Interagency Data Transparency Commission report
https://dir.texas.gov/resource-library-item/idtc-final-reportpdf

Texas Electronic State Business Daily (ESBD)
https://www.txsmartbuy.com/ShopFlow/help/docs/esbd_manual.pdf

Texas Statewide Data Exchange Compact | Texas Department of Information Resources
https://dir.texas.gov/office-chief-data-officer/texas-statewide-data-exchange-compact

Federal Data Strategy Ethics Framework
https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf

Texas Open Data Portal
https://data.texas.gov/

Texas Data Portals Resource Guide
https://data.texas.gov/dataset/Texas-Data-Portals-Resource-Guide/wxtw-nqep

TX-RAMP Eligibility and Requirements | Texas Department of Information Resources
https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp/tx-ramp-eligibility

Data Center Services | Texas Department of Information Resources
https://dir.texas.gov/shared-technology-services/data-center-services

The determinants of organizational change management success: Literature review and case study
https://journals.sagepub.com/doi/epub/10.1177/18479790211016273

What is Change Management? Organizational, Process, Definition & Tools | ASQ
https://asq.org/quality-resources/change-management

Texas Data Literacy Program
https://dir.texas.gov/tdlp

Authors and Contributing Agencies

Authors

Ricky Beverlin, Data Management Intern, Texas Department of Information Resources
Monica Smoot, Texas Department of Information Resources
Stacey Lewis, Texas Department of Information Resources
Grant Caldwell, Texas Commission for Environmental Quality
Brady Cox, Public Utility Commission of Texas
Jennie Hoelscher, Texas Department of Information Resources

Other Contributing Agencies

Texas Department of Insurance
Texas Comptroller of Public Accounts
Texas Department of Agriculture
Texas Education Agency
Texas Health and Human Services Commission