

# DIR Discover 2023

Privacy Breakout Session  
September 21, 2023



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/hashtag/DIRisIT)

# Today's Agenda

- Part I – 9:00-10:15
  - Introduction
  - FIPPS for Texas Public Sector Entities
  - Preparing Website Privacy Notices
- Break – 10:15-10:30
- Part II – 10:30-11:45
  - Data Breach Response and Notifications
  - Privacy Officer Roundtable
  - Privacy Resources and Networking Opportunities

# Fair Information Practice Principles in Texas

Jennie Hoelscher

DIR Privacy Officer & Assistant General Counsel



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/TexasDIR)

# Fair Information Practice Principles (FIPPs)

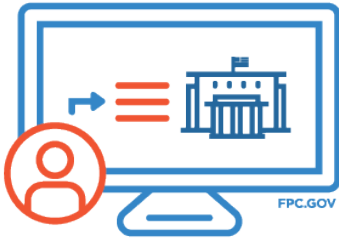
# Some Historical Background

## How were the FIPPs developed?

- In 1973, the Department of Health, Education, and Welfare Advisory Committee issued a report identifying Fair Information Practice Principles (FIPPs). That report articulated ideals for the way governments process the personal information they maintain about constituents.
- Those FIPPs have evolved and have been incorporated in varying degrees into federal and U.S. state laws as well as the policies of many private organizations around the world.
- Numerous other organizations have created their own FIPPs to guide their organizations privacy program.



# Overview of Common FIPPs



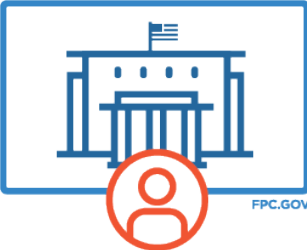
**ACCESS AND AMENDMENT**



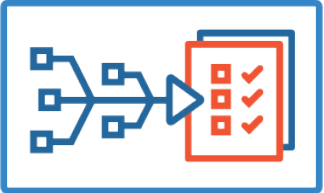
**ACCOUNTABILITY**



**AUTHORITY**



**INDIVIDUAL PARTICIPATION**



**MINIMIZATION**



**PURPOSE SPECIFICATION AND USE LIMITATION**



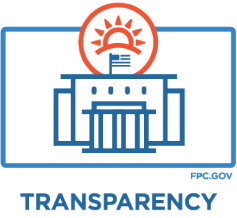
**QUALITY AND INTEGRITY**



**SECURITY**



**TRANSPARENCY**



# Transparency

**Governmental bodies should be transparent about how they collect, use, maintain, and share the personal information they possess about their constituents.**

- Provide clear and accessible privacy notices.
- Make privacy notices easy to read.
- Keep privacy notices up to date.
- Notify constituents of any material changes to privacy practices.





# Individual Participation

**Governments should, to the extent practicable, seek individual consent for the creation, collection, use, or sharing of PII. Governments should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.**

- Designate a resource that constituents may reach out to if they have privacy questions or concerns and identify that resource in the privacy notice.



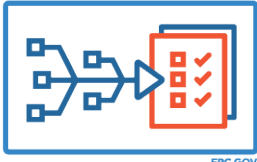


PURPOSE SPECIFICATION  
AND USE LIMITATION

# Purpose Specification and Use Limitation

Governments should provide notice of the specific purpose for which PII is collected and should only use, process, maintain, and share PII for a purpose that is explained in the notice, is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

- Identify within the privacy notice the purposes for using the personal information collected.
- Ensure policies and procedures exist to prevent using information beyond the purposes specified when the information was collected.



MINIMIZATION

# Minimization

Governmental bodies should only collect, use, process, maintain, and share PII that is directly relevant and necessary to accomplish an authorized purpose. Governmental bodies should only maintain PII for as long as is necessary to accomplish the purpose.

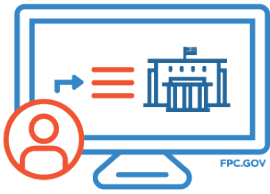
- Before collecting any PII, consider what information is necessary to perform the service or function and do not collect anything beyond what is necessary.
- Consider whether records retention schedules are consistent with the organization's need to retain personal information and adjust if needed
- Follow records retention schedules to ensure that PII is deleted or destroyed when the schedule allows.



# Quality and Integrity

Governmental bodies should collect, use, maintain, and share PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

- Consider implementing processes to ensure the ongoing accuracy of data and only process data known to be accurate.



ACCESS AND  
AMENDMENT

# Access and Amendment

Governmental bodies should provide individuals with appropriate access to their personal identifying information and appropriate opportunity to correct or amend their PII.

- Open records laws generally require governmental entities to provide access unless an exemption applies.
- Establish clear, simple procedures for individuals to access their PII and to correct it if needed.



ACCOUNTABILITY

# Accountability

**Governmental bodies should be accountable for complying with applicable privacy requirements, and should appropriately monitor, audit, and document compliance.**

- Establish procedures to monitor compliance with privacy policies.
- Review access controls to ensure only those with a need to access PII are able to do so.

**Governmental bodies should also define the roles and responsibilities with respect to PII for all employees and contractors and should provide appropriate training to those with access to PII.**



# Security

**Governmental bodies should establish administrative, technical, and physical safeguards to protect personal information.**

- Coordinate with the Information Security Officer to ensure that adequate security controls are placed on systems that contain PII.
- Ensure that only those employees and contractors who need access to PII have it.





# Authority

**Governmental bodies should only collect, use, maintain, or share PII if they have authority to do so, and should identify this authority in the appropriate notice.**

- Review the data the organization collects and determine what authority (if any) exists for collecting it.
- Consider revising data collection practices if authority to collect specific data is not clear.





# **How Texas Incorporates the FIPPs**

# The Texas Data Privacy and Security Act Applies FIPPs to Certain Texas Businesses in the Private Sector

Access and Correction

Individual Participation, including Deletion and Opt-Out

Minimization

Security Controls

Transparency

Purpose Specification & Use Limitation

Accountability

HB 4 “does not apply to...a state agency or a political subdivision of this state.”

# The Texas Medical Records Privacy Act Applies FIPPs to Covered Entities Possessing Protected Health Information

Access and Correction

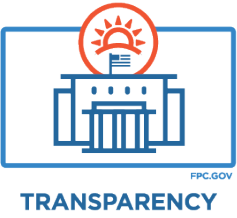
Individual Participation

Purpose Specification & Use Limitation

Transparency

Accountability

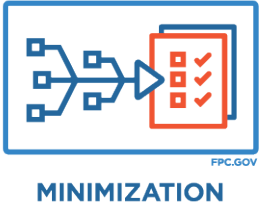
Governmental bodies may qualify as covered entities under the TMRPA if they possess, process, or obtain protected health information.



# Transparency

## Privacy Notices – Texas Government Code § 559.003(b)

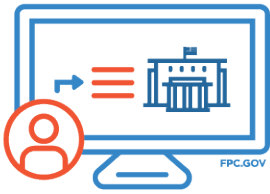
- State governmental bodies that collect information about an individual must post a privacy notice on their Internet site that explains what information is being collected, including what information is being collected by means that are not obvious.



# Minimization

## Review of Data Collection Practices – Texas Government Code § 2054.112

- When delivering services through the Internet, state governmental bodies shall review their data collection policies and determine if the personal information collected about individuals is necessary. State governmental bodies shall eliminate any unnecessary collection of information.



ACCESS AND  
AMENDMENT

# Access and Amendment

## Right of Access –

### Texas Government Code § 559.002, .003

- An individual is entitled to be informed about information that a state governmental body collects about the individual unless the state governmental body is allowed to withhold the information from the individual under the Public Information Act. The individual is entitled to receive and review the information.

## Right to Correction –

### Texas Government Code § 559.004

- A state governmental body must establish a procedure for individuals to have the governmental body amend incorrect information about the individual that the government possesses.



ACCOUNTABILITY

# Accountability

## Employee Data Use Agreements – Texas Government Code § 2054.135

- State governmental bodies shall develop a data use agreement for employees of the agency who handle sensitive information, including financial, medical, personnel, or student data. Employees handling sensitive information must sign the agreement and receive appropriate training about the organization's related policies and procedures. The agreement should outline the employees' responsibilities related to the secure handling of sensitive data.





# Security

## Information Security Plans – Texas Government Code § 2054.133

- State governmental bodies shall develop, and periodically update, an information security plan for protecting the security of the agency's information.

## Security Controls for State Agency Data – Texas Government Code § 2054.138

- State governmental bodies shall include provisions in contracts with vendors that require the vendors to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data.

# Questions?



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/TexasDIR)

# Drafting Website Privacy Notices

**Meghan Frkuska**

Chief Privacy Officer, Texas Department of Public Safety

**Jennie Hoelscher**

DIR Privacy Officer & Assistant General Counsel



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/TexasDIR)

# Privacy “Notices” vs. Privacy “Policies”

## Privacy Notice

An external-facing document that explains to constituents how an agency collects, uses, shares and manages personal information.

## Privacy Policy

An internal-facing document outlining an agency’s procedures for how employees protect and manage personal information.

### Privacy and Security Policy

The Texas Department of Information Resources maintains this website as a public service. This policy describes DIR's privacy and security practices regarding information collected from visitors to the site, including what information is collected and how that information is used. The policy applies to all pages beginning with [www.dir.state.tx.us](http://www.dir.state.tx.us), [www2.dir.state.tx.us](http://www2.dir.state.tx.us), [www.dir.texas.gov](http://www.dir.texas.gov), and [www2.dir.texas.gov](http://www2.dir.texas.gov).

#### 9.1 CONFIDENTIAL INFORMATION

DIR Employees sign the [Nondisclosure and Conflict of Interest Certification form](#) on beginning employment and annually thereafter. In accordance with this form, employees shall not disclose confidential information belonging to DIR or other entities obtained in the course of their employment to individuals not subject to a DIR-specific non-disclosure agreement. An employee may disclose confidential information to an employee of another state agency if there is a legitimate business reason for doing so. Any requests for confidential documents are subject to DIR's Public Information Policy.

Employees shall not use confidential information belonging to DIR or other entities obtained in the course of their employment, including confidential information acquired from business transactions, for the purposes of advancing any private interest or otherwise for personal gain.

# Why Are Privacy Notices Important?



Required by law



Gives constituents a clear picture about how their personal data is collected and used



Establishes trust among our constituents

# Roadmap

## Steps to Creating a Website Privacy Notice

- Determine the PII collected by the organization (factual due diligence);
- Determine privacy laws applicable to organization's data (legal due diligence);
- Draft the policy
- Confer with the data controllers to ensure accuracy;
- Publish policy; and
- Regularly review and update policy.

## Regular Review of the Policy and Updating as Needed

## Consequences for Noncompliance





A dark blue background with a network diagram consisting of light blue lines and circular nodes of varying sizes, some of which are highlighted with a larger, darker blue circle.

**Determine the  
PII Collected**



# What You Need to Know

What authority does your organization have to collect data?

What personal information does the organization collect?

How is it collected?

What is the purpose for its collection?

Is personal information shared outside the governmental body? If so, with whom? Is it sold?

How is the personal information secured and protected?

# What Personal Information Is Your Governmental Body Collecting About Constituents?

- Coordinate with your Data Management Officer, IT Department, and individual teams to obtain a clear picture of the data within the organization.
- Determining what PII is collected may require involvement from all business teams within the organization.
- Teamwork makes the dream work, the dream here being transparency about your organization's collection and use of personal information.





# **Determine Applicable Laws and Regulations**

# State Government Privacy Policies

## Texas Government Code, chapter 559

State governmental bodies that collect information about individuals online must:

- Post a privacy notice on their website.
- Identify the information collected through the site about the individual.
- Identify the information collected about the computer network location or identity of a user of the site, including what information is being collected by means that are not obvious.
- Provide individuals access to review their personal information.
- Provide a simple, no-cost procedure to correct personal information about the individual.





# Texas Administrative Code 206.52

- Each state agency must publish a privacy notice on its home page and all key public entry points or its site policies page.
- The privacy notice must describe the practices employed by the state agency to protect personal identifying information and be consistent with the State Website Linking and Privacy Policy published on DIR's website.
- Any web-based form on a state agency's website that requests information from the public must have a link to the state agency's website privacy notice.



# Sector Specific State Laws Requiring Privacy Notices in Certain Instances

Some laws require specified privacy notices for certain types of governmental units or certain types of data:

- Municipally-owned utilities that collect social security numbers
- Texas Fusion Center (law enforcement repository for Homeland Security information)
- Entities collecting or biometric identifiers in certain instances

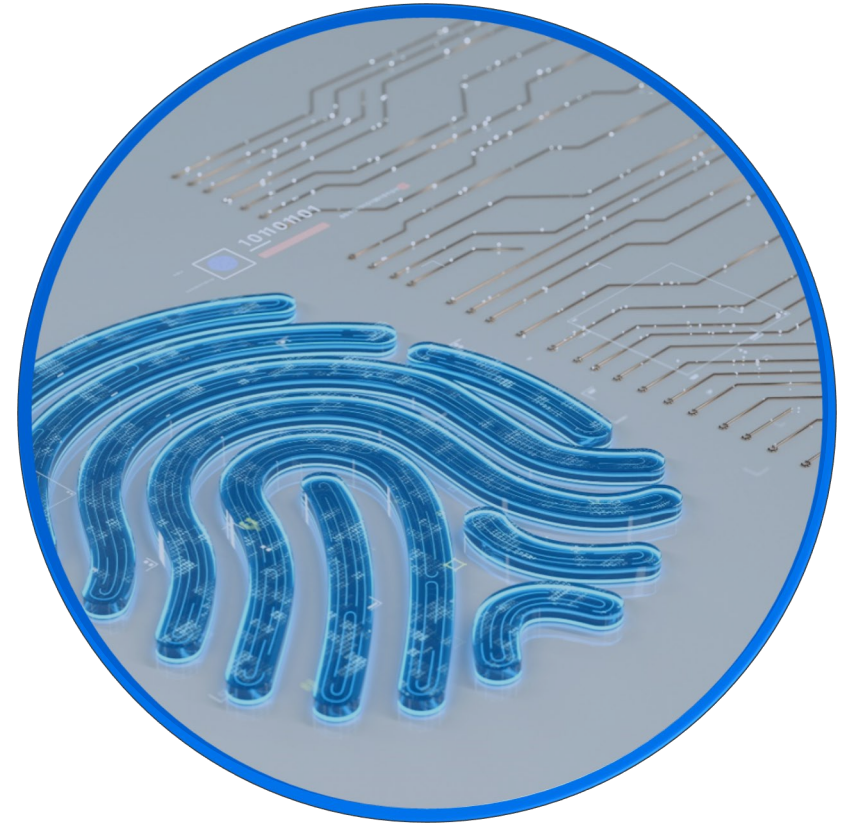
**Confer with legal counsel to ensure the privacy notice includes all applicable requirements and notices.**

# Restrictions on Use of Individual-Identifying Information

## Texas Government Code, chapter 2062

A state agency may not collect, retain, or disseminate biometric identifiers without the individual's express written or electronic consent.

Biometric identifiers include retina or iris scans, fingerprints, voiceprints, or records of hand or face geometry.





# Federal Laws and Regulations Requiring Privacy Notices for Certain Market Sectors



HIPAA – Health Insurance Portability and Accountability Act



FERPA – Family Educational Rights and Privacy Act



GLBA – Gramm-Leach Bliley Act

# Other Possible Sources of Law



## Ordinances Governing Municipalities or Counties

- Some municipalities have adopted ordinances governing how a city collects and processes data and what notice is required before doing so.



## General Data Protection Regulation (GDPR) – European Union privacy law

- If your governmental body processes personal identifying information of residents of the EU, consult with your legal counsel about the requirements of the GDPR that may be applicable to the organization.



## Children's Online Privacy Protection Act (COPPA)

- If your governmental body collects personal identifying information from children under age 13, consult with your legal counsel about COPPA requirements that may be applicable to the organization.

# NIST Privacy Framework

<p><b>COMMUNICATE-P (CM-P):</b> Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.</p>	<p><b>Communication Policies, Processes, and Procedures (CM.PO-P):</b> Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.</p>	<p><b>CM.PO-P1:</b> Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.</p> <p><b>CM.PO-P2:</b> Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.</p>
---	--	---

# NIST 800-53

## PT-5 **PRIVACY NOTICE**

Control: Provide notice to individuals about the processing of personally identifiable information that:

- a. Is available to individuals upon first interacting with an organization, and subsequently at *[Assignment: organization-defined frequency]*;
- b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
- c. Identifies the authority that authorizes the processing of personally identifiable information;
- d. Identifies the purposes for which personally identifiable information is to be processed; and
- e. Includes *[Assignment: organization-defined information]*.



**Draft the Privacy Notice**

# What to Include in a Privacy Notice

The content of a privacy notice will depend on the specific personal information an organization collects, how it uses that information, and the relevant laws applicable to the organization. Items to consider including in a notice are:

- Types of personal information collected
- How personal data is used and shared
- Where personal data is stored and for how long
- How personal data is protected
- Procedures for accessing and amending personal information
- Intersection of privacy practices with the Public Information Act
- Contact information for questions or complaints
- Right to withdraw consent (if applicable)
- Disclaimer for links to other websites
- Effective date or date of most recent update

# Best Practices for Drafting a Privacy Notice

Keep it simple.

Avoid legalese.

Break up the content into sections.

Use headers and bullet points.

Use layers if the content is lengthy.





# Consider a Layered Privacy Notice if Content is Lengthy

- + What information do we collect from you?
- + Why do we collect this information?
- How do we protect this information?

We have taken steps to safeguard our data and prevent unauthorized access to information maintained by us.

These measures are designed to prevent corruption of data, block unknown or unauthorized access to our systems and information, and to provide reasonable protection of information in our possession.



# Privacy Notice Templates



## HIPAA

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html>



## FERPA

<https://studentprivacy.ed.gov/annual-notices>



## GLBA

[https://www.sec.gov/files/rules/final/2009/34-61003\\_modelprivacyform.pdf](https://www.sec.gov/files/rules/final/2009/34-61003_modelprivacyform.pdf)



**Confer With Business  
Owners To Ensure  
Accuracy**



**Publish Privacy Notice**

# Notify Constituents of Any Material Changes?

## Possible Methods to Notify:

- Include an Update Clause in the Privacy Notice
- Send an email updating constituents about the changes to the privacy policy.
- Use a pop-up notice on the website.

Different laws have varying requirements about when entities must notify their users about material changes to the privacy notices.

Consult your legal counsel to determine which notification requirements apply to your organization.

# Post a Link to the Privacy Notice on the Home Page of the Website

State agencies must post a privacy notice on their home page and must also include a link to the privacy notice on any web-based form that collects personal information.

## About Us

[About Texas.gov](#)

[Site Policies](#)

[Privacy Policy](#)

[Sitemap](#)

©2023 Texas Department of Information Resources

[Privacy & Site Policies](#)

[Accessibility](#)

[Ethics Policy](#)

[Public Information Requests](#)



**Review and Update  
Notice Regularly**




# Change Is Inevitable

## Business practices change over time.

- An organization may find a need to collect additional personal information to better effectuate a government service or more securely protect its IT systems.

Anytime any organization changes the personal information that it collects, how it uses or shares that information, or how it protects it, the privacy notice must be reviewed and updated.



# Consequences for Not Complying with Privacy Notices

# What Are the Consequences For Failing To Comply With Privacy Notice Laws?

## Legal Action by Entities with Jurisdiction to Enforce Privacy Laws

- The FTC and DOJ have brought actions against governmental bodies whose actual data collection and use practices are contrary to the privacy notice posted on the governmental body's website.

## Reputational Harm

- If governments handle data contrary to the promises made in a privacy notice, constituents may be reluctant to continue doing business with those entities, or at least reluctant to do business online.



# Questions?



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/TexasDIR)

# Data Breach Notification Under the Texas Identity Theft Enforcement and Protection Act

Jennie Hoelscher

DIR Privacy Officer & Assistant General Counsel



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/hashtag/DIRisIT)

# Data Breaches Happen

547

Data breaches reported to the Texas Office of the Attorney General during the past year (9/9/22 – 9/8/23)

1,802

Data breaches reported across the United States during 2022, as reported by the Identity Theft Resource Center



# Numerous Laws Govern Data Breach Notifications

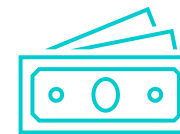
Every state in the U.S. has its own data breach notification statute. Most are similar, but differences exist between the state laws.



Certain market sectors have additional federal breach notification requirements that vary by applicable law. For example:



**HIPAA** requires covered entities to notify impacted individuals following the release of the unsecured protected health information.



**Publication 1075** requires governmental entities to notify taxpayers when their federal tax information is subject to unauthorized access or disclosure.

<https://iapp.org/resources/article/state-data-breach-notification-chart/>

# The Texas Data Breach Notification Law

## The “Texas Identity Theft Enforcement and Protection Act,” chapter 521 of the Business and Commerce Code

- The Act requires businesses operating in Texas to protect the sensitive personal information they collect and maintain from unlawful use or disclosure.
- If a breach occurs that results in the unauthorized acquisition of that sensitive personal information, businesses must notify the individuals whose personal information was acquired.



# Also Applicable to Governmental Bodies

## Texas Government Code § 2054.603

- State agencies and local governments that own, license, or maintain computerized data that includes sensitive personal information must comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state.



# Questions To Answer During a Breach

- 1 Has the individual notification requirement been triggered?
- 2 What does the notification need to include?
- 3 What is the deadline for sending notification?
- 4 How should the notification be sent?
- 5 Do we need to report the breach to other governmental entities?





**Has the Notification  
Requirement Been  
Triggered?**



# Does the Incident Involve Sensitive Personal Information (SPI)?

The Act defines SPI as a first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- i. social security number;
- ii. driver's license number or government-issued identification number; or
- iii. account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.





# Health-Related Sensitive Personal Information

SPI also includes information that identifies an individual and relates to:

- i. the physical or mental health or condition of the individual;
- ii. the provision of health care to the individual; or
- iii. payment for the provision of health care to the individual.



# Differing Definitions of Sensitive Personal Information

## Other states define SPI differently.

Some states include consider additional information to be SPI, such as:

- biometric data,
- home address,
- telephone number,
- place of employment,
- employee identification number, or
- mother's maiden name.

If the data of a resident of another state is compromised, review the resident's state data breach reporting law to determine whether additional notification is required.

# Is There a Breach of System Security?

A “breach of system security” is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

Work with your IT Department and/or relevant contractors or vendors to determine the nature of the breach and whether sensitive personal information was accessed.

## Elements required for a breach under the Act:

- Computerized data
- Reasonable belief that SPI was acquired by a person not authorized
- Compromises the security, confidentiality, or integrity of SPI





**What Should The  
Notification to Impacted  
Individuals Include?**

# Minimal Content Requirements Under Texas' Law

A governmental body  
"shall disclose any breach  
of system security..."





# Other States Require More Detail

[NAME OF INSTITUTION / LOGO] _____ Date: [insert date]	
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Website]



# HIPAA Notification Content Requirements

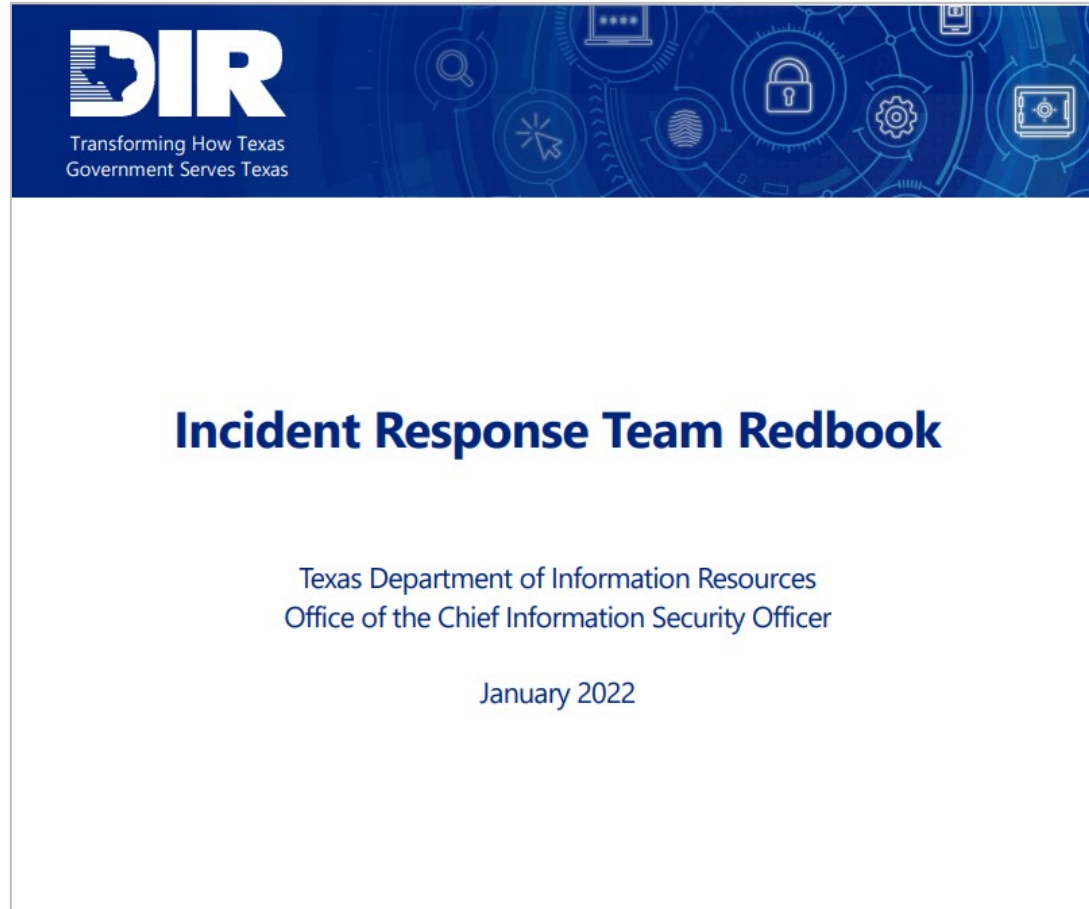
- A brief description of the breach.
- A description of the types of information involved in the breach.
- The steps affected individuals should take to protect themselves from potential harm.
- A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches.
- Contact information for the covered entity (or business associate, as applicable).



# Publication 1075 Notification Content Requirements

- The date of the unauthorized inspection or disclosure of federal tax information
- The rights of the taxpayer under IRC § 7431A

# A Template for Data Breach Notification Letters



<https://dir.texas.gov/resource-library-item/texas-dir-incident-response-team-redbook-template>

# Who Signs The Breach Notification Letter Sent To Impacted Individuals?

- Elected or appointed official or Executive Director or administrative leader?
- Privacy Officer?
- Head of the department directly responsible for the breached system?
- Head of IT?

The law does not specify who signs and sends the letter. Making this decision can take time and delay the notification process. Governmental bodies should consider this question in advance – before a breach occurs – to avoid delay in the notification process.

**By When Must The  
Notice To Impacted  
Individuals Be Sent?**

# Timing of Individual Notification

Without unreasonable delay.

Not later than 60 days after the governmental body determines that the breach occurred.

- OAG notification, when required, must be sent within 30 days. Governmental bodies may want to provide earlier individual notice in those instances.

**Exceptions to the 60-day deadline:**

- Law enforcement requests a delay to avoid impeding a criminal investigation.
- The governmental body needs more time to “determine the scope of the breach and restore the reasonable integrity of the data system.”



# When Did the Governmental Body “Determine That the Breach Occurred?”



A security incident occurs involving the unauthorized access of sensitive personal information.



Governmental body receives information about a possible security incident.



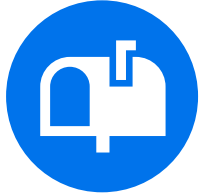
Governmental body confirms an unauthorized user accessed SPI.





# How Should The Notice Be Sent?

# Generally Speaking, First Class Mail



Written notice at the last known address of the individual.



Electronic notice, if the individual has consented pursuant to federal law.



If the cost would exceed \$250,000, the number of affected exceeds 500,000, or insufficient contact information exists:

- Email
- Conspicuous posting on website
- Notification through major statewide media

# Or Follow Your Own Policy

The law allows a governmental body who maintains its “own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.”

Should you consider an information security policy that establishes notification procedures for your governmental body?





**What Other Entities  
Must Be Notified,  
and By When?**

# Reporting to DIR

<https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/sb-271-security-incident>



Within 48 hours of the discovery of the security incident, notify the Department of Information Resources.



Notification occurs through SPECTRIM, the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management.



Texas Department of Information Resources

# Reporting to the Office of the Attorney General

<https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting>



Governmental bodies must notify the Office of the Attorney General if they determine that a breach involves at least 250 residents of this state.



Notification is required as soon as practicable and not later than 30 days after the date the governmental body determined that the breach occurred.



**Data Breach Report**

THIS FORM SHOULD BE COMPLETED ONLY BY THE OWNER, MANAGER, ATTORNEY, OR AGENT AUTHORIZED BY THE BUSINESS OR ORGANIZATION TO SUBMIT A DATA BREACH REPORT AS REQUIRED BY CHAPTER 521, TEXAS BUSINESS AND COMMERCE CODE.

**NOTICE TO CONSUMERS:**  
IF YOU ARE AN INDIVIDUAL THAT HAS BEEN NOTIFIED OF A DATA BREACH, AND/OR ARE NOT AN AUTHORIZED REPRESENTATIVE OF THE BUSINESS OR ORGANIZATION EXPERIENCING A DATA BREACH, PLEASE SUBMIT YOUR INFORMATION VIA A [CONSUMER COMPLAINT FORM](#).

**NOTICE OF LEGISLATIVE CHANGES:**  
Effective September 1, 2023, all required data breach notices submitted to the Office of the Attorney General (a) must be submitted **not later than the 30th day** after the date on which the breach is discovered; and (b) those notices (and supplemental reports) **must be submitted electronically** using this reporting form.

**PART A - IDENTIFYING INFORMATION OF BUSINESS OR ORGANIZATION THAT EXPERIENCED THE BREACH**

1. Name of Business or Organization That Owns or Licenses the Data Subject to the Breach

\* Business or Organization Name

2. Your Relationship to the Business or Organization That Experienced the Breach

\* Type of Relationship

-- Select One --



# OAG Posting of Data Breach Reports

<https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage>

## Data Security Breach Reports

Details including number of affected Texans and whether notice was provided to them may change after a report is listed here.

Search:

ENTITY OR INDIVIDUAL NAME	ENTITY OR INDIVIDUAL ADDRESS	ENTITY OR INDIVIDUAL CITY	ENTITY OR INDIVIDUAL STATE	ENTITY OR INDIVIDUAL ZIP CODE	TYPE(S) OF INFORMATION AFFECTED	NUMBER OF TEXANS AFFECTED	NOTICE PROVIDED TO CONSUMERS (Y/N)	METHOD(S) OF NOTICE TO CONSUMERS
---------------------------	------------------------------	---------------------------	----------------------------	-------------------------------	---------------------------------	---------------------------	------------------------------------	----------------------------------



# Reporting to Consumer Reporting Agencies

If a governmental body is required to notify more than 10,000 persons of a breach, the governmental body must notify nationwide consumer reporting agencies.

**EQUIFAX**<sup>®</sup>

 experian<sup>™</sup>

TransUnion<sup>®</sup> 

# Reporting Required Under Sector-Specific Laws

Sector-specific laws require reporting to other governmental entities in certain circumstances. Examples include:

- HIPAA requires notification to the Secretary of Health and Human Services in certain instances.
- If election data is disclosed, state law requires notification to the Texas Secretary of State.
- Publication 1075 requires notification to the Treasury Inspector General for Tax Administration in certain circumstances when federal tax information is disclosed.

# Prior Preparation Prevents Poor Performance



No entity is immune from the risk of a data breach.



Governmental bodies must prepare to respond to an eventual data breach. Considering the notification procedures in advance will result in better outcomes and reduce stress when the inevitable occurs.

And thank you to those entities who have experienced the data breach notification journey and are willing to share their knowledge to help light the way.

# Questions?

Jennie Hoelscher  
DIR Privacy Officer  
[Jennie.Hoelscher@dir.texas.gov](mailto:Jennie.Hoelscher@dir.texas.gov)



Texas Department of Information Resources

Transforming How  
Texas Government  
Serves Texans

[dir.texas.gov](http://dir.texas.gov) | [@TexasDIR](https://twitter.com/TexasDIR) | [#DIRisIT](https://twitter.com/DIRisIT)

# Privacy Officer Panel



Meghan Frkuska  
Chief Privacy Officer  
Texas Department of Public Safety



Emilie Schulz  
Data Privacy Officer  
Texas Department of Transportation



A dark blue background with a network diagram consisting of white dots connected by thin white lines, representing a network or data structure.

# Privacy Resources and Networking Opportunities

# International Association of Privacy Professionals (IAPP)

- A nonprofit organization devoted to providing a forum for privacy professionals to share best practices, track trends, and provide education and guidance on the field of information privacy.
- Government Membership is \$100 annually.
- <https://iapp.org/>

The logo for the International Association of Privacy Professionals (IAPP) is displayed in a bold, lowercase, green sans-serif font. The background of the logo area is a dark blue gradient with a network of white lines and dots, suggesting a global or interconnected theme.

# IAPP Resources

## US State Privacy Legislation Tracker

Last Updated: 15 September 2023

[View Chart](#)

[View Map](#)

[View Enacted Laws](#)

State-level momentum for comprehensive privacy bills is at an all-time high. The IAPP Westin Research Center actively tracks the proposed and enacted comprehensive privacy bills from across the U.S. to help our members stay informed of the changing state privacy landscape. This information is compiled into a [map](#), a [detailed chart](#) identifying key provisions in the legislation, and [links](#) to enacted state comprehensive privacy laws.



## Web Conference: Generative AI Governance 101 — A masterclass for privacy pros

This web conference addresses the regulatory landscape for AI, approaches companies are taking to govern generative AI tools, and more. [Read More](#)

## 10 steps to undertaking a privacy impact assessment

When developing or reviewing a project, consider the need for a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy and makes recommendations to manage, minimise or eliminate privacy impacts.

We recommend that organisations conduct PIAs as part of their risk management and planning processes. While each project is different, a PIA should generally include the following 10 steps.

### 1. Threshold assessment

Ask if any personal information will be collected, stored, used or disclosed in the project. If the answer is yes, a PIA is usually necessary. Keep a record of this threshold assessment.

### 2. Plan the PIA

Consider the scope of your assessment, who will conduct it, the timeframe, budget and who will be consulted.

### 3. Describe the project

Prepare a project description to provide context for the PIA project. This should be brief, but sufficiently detailed to allow external stakeholders to understand the project.

### 4. Identify and consult with stakeholders

Identify the project stakeholders. Consulting them can help to identify new privacy risks and concerns, better understand all risks.

Information flows, and disclosed, have access.

### 5. Compliance

Privacy. Consider information organisation. Even

if the project appears to be compliant with privacy legislation, there may be other privacy considerations that need to be addressed such as community expectations.

### 7. Privacy management — considering risks

Consider options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis.

### 8. Recommendations

Make recommendations to remove, minimise or mitigate the risks identified through the privacy impact analysis. Include a timeframe for implementing the recommendations.

### 9. Report

Prepare a report that sets out all the PIA information. It should be a practical document that can easily be interpreted and applied. The OAIC encourages the publication of PIA reports and has developed a [PIA tool](#) to help you conduct a PIA, report its findings and respond to recommendations.

### 10. Respond and review

Monitor the implementation of the PIA recommendations. A PIA should be regarded as an ongoing process that does not end with preparation of a report. It is important that action is taken to respond to the recommendations in the report, and to review and update the PIA, particularly if issues arise during implementation.

See our [Guide to undertaking privacy impact assessments](#), [e-learning course](#) and [PIA tool](#) for more information.



OAIC

# IAPP Certification Programs



**CIPP**

Laws and regulations

The global standard for the go-to person for privacy laws, regulations and frameworks



**CIPM**

Operations

The first and only privacy certification for professionals who manage day-to-day operations



**CIPT**

Technology

The industry benchmark for IT professionals worldwide to validate their knowledge of privacy requirements

iapp

# Government Technology

A magazine published by e.Republic, a research company focused on public sector innovation.

- Webinars
- Articles on privacy current events



How State Governments Can Address the Growing  
**DEMAND FOR DIGITAL PRIVACY**

Overview

December 9  
11AM PT, 2PM ET

[WATCH NOW](#)



K-12 EDUCATION

**Proposed Federal Privacy Laws Could Affect Schools**

Congress is considering two proposed laws governing Internet use — one prohibiting companies from collecting data on youth without their consent, and another requiring social media to have parental controls.

August 21, 2023 - Aaron Gifford

**verizon**  
Content from Verizon

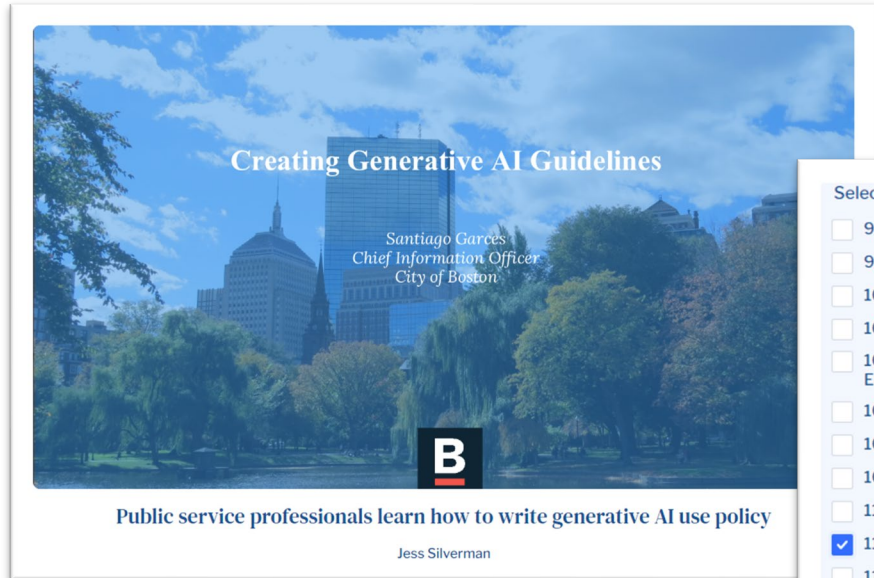
- 1 How a Smart Connected Campus Enhances the Student Experience
- 2 Zero Trust Security for K-12 and

<https://www.govtech.com/tag/privacy>





# Innovate-us



Select which workshops you would like to sign up for: \*

- 9/20: Modernizing Unemployment Benefits: A Hands-On Workshop for States
- 9/28: To Post or Not to Post: The Highs and Lows of Government Social Media
- 10/5: Program Evaluation Series: Understanding Program Evaluation Essentials
- 10/6: An Introduction to AI for the Public Sector
- 10/12: Program Evaluation Series: Navigating Stakeholder and Community Engagement in Program Evaluation
- 10/19: Program Evaluation Series: Crafting Logic Models and Developing Indicators
- 10/24: Data Series: An Introduction to Data and Its Reuse
- 10/26: An Ethics Ecosystem for AI and Big Data: Why? What? How?
- 11/1: Data Series: The Science of Data Questions and Exploring Data Sources
- 11/2: How to Write a Generative AI Policy for Your Jurisdiction
- 11/6: Data Series: Data Collaboration and Governance
- 11/14: What Works? Using Tools to Find Solutions to Public Policy Problems
- 11/29: Human-Centered Design Series: Introduction to Human-Centered Design for the Public Sector
- 11/30: Bringing AI and Tech Talent into Government
- 12/6: Human-Centered Design Series: Putting the 5 Key Phases into Action
- 12/7: How to Use Generative AI in Government: Text Tools
- 12/13: Human-Centered Design Series: Human-Centered Design in Government
- 12/14: How to Use Generative AI in Government: Image Tools
- Date TBD: Trends in AI and the Impact for the Public Sector

<https://innovate-us.org/>





# Connect with Texas Public Sector Privacy Professionals

Interested in joining our network of state privacy professionals? Ask questions, learn from other agency privacy leaders, and share your privacy practices among a supportive group of privacy pros.

To join our privacy network, send your name, title, agency, and email address to:

[Jennie.Hoelscher@dir.texas.gov](mailto:Jennie.Hoelscher@dir.texas.gov)

