TEXAS DEPARTMENT OF INFORMATION RESOURCES

Incident Response Team Redbook

June 2020

Contents

Introduction

When a privacy or information security incident occurs, it is imperative that the agency follow documented procedures for responding to and processing the incident. An Incident Response Team (IRT) Redbook is intended to contain the procedures and plans for such incidents when they occur. The Redbook should be in both hard copy and electronic formats and be readily available to any standing member of the IRT team.

Two principles guide the establishment of the Redbook. First, is that every agency must establish in advance and maintain a plan for responding to an incident. Second, every agency must test and update the operation of the plan periodically to ensure that it is appropriate and functional.

This is a template and is intended to be a framework for state agencies in creating their own Redbook and should be modified and completed to meet the business needs of the agency.

Defined terms are in **bold** print.

SECTION 1

Glossary and Acronyms

1.1 Glossary

Admissible Evidence: evidence that is accepted as legitimate in a court of law, *see* Chain of Custody.

Authentication: security measure designed to establish the validity of a transmission, message, or originator, or the identity confirmation process used to determine an individual's authorization to access data or computer resources.

Authorized User: a person granted certain permissions to access, manage, or make decisions regarding an information system or the data stored within.

Authorized Use and Disclosure: a permissible action or use of **Confidential Information**.

Authorization: the act of granting a person or other entity permission to use data or computer resources in a secured environment.

Availability: The security objective of ensuring timely and reliable access to and use of information.

Breach: an impermissible use or disclosure by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of **Confidential Information** such that the use or disclosure poses a significant risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Depending upon applicable law, "Breach" may for example mean:

1) HIPAA Breach of Protected Health Information ("PHI"). With respect to PHI pursuant to HIPAA Privacy and Breach Notification Regulations and regulatory guidance any unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Regulations is presumed to be a Breach unless a Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Compromise will be determined by a documented Risk Assessment including at least the following factors:
    a. The nature and extent of the **Confidential Information** involved, including the types of identifiers and the likelihood of re-identification of PHI;
    b. The unauthorized person who used or to whom PHI was disclosed;
    c. Whether the Confidential Information was actually acquired or viewed; and
    d. The extent to which the risk to PHI has been mitigated.

   With respect to PHI, a "Breach" pursuant to HIPAA Breach Regulations and regulatory guidance *excludes*:
    a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority, and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations.
    b. Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate location to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement as

defined by HIPAA in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations

c. A disclosure of PHI where a Covered Entity or Business Associate demonstrates a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, pursuant to HIPAA Breach Regulations and regulatory guidance.

2) Breach in Texas. Breach means "Breach of System Security," applicable to electronic Sensitive Personal Information (SPI) as defined by the Texas Identity Theft Enforcement and Protection Act, Business and Commerce Code Ch. 521, that compromises the security, confidentiality, or integrity of Sensitive Personal Information. Breached SPI that is also PHI may also be a HIPAA breach, to the extent applicable.
3) Any unauthorized disclosure as defined by any other law and any regulations adopted thereunder regarding **Confidential Information**.

Business Continuity Plan: the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Chain of Custody: refers to the application of the legal rules of evidence and its handling.

Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. This includes any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) that consists of or includes any or all of the following:

1) Federal Tax Information, sourced from the Internal Revenue Service (IRS) under an IRS data sharing agreement with the agency;
2) Personal Identifying Information;
3) Sensitive Personal Information;
4) Protected Health Information, whether electronic, paper, secure, or unsecure;
5) Social Security Administration data, sourced from the Social Security Administration under a data sharing agreement with the agency;
6) All non-public budget, expense, payment, and other financial information;
7) All privileged work product;
8) Information made confidential by administrative or judicial proceedings;
9) All information designated as confidential under the laws of the State of Texas and of the United States, or by agreement; and
10) Information identified in a contract or data use agreement to which an agency contractor specifically seeks to obtain access for an Authorized Purpose that has not been made public.

Confidentiality: The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Containment: the process of preventing the expansion of any harmful consequences arising from an Incident.

Contingency Management Plan: a set of formally approved, detailed plans and procedures specifying the actions to be taken if or when particular circumstances arise. Such plans should include all eventualities ranging from key staff absence, data corruption, loss of communications, virus infection, partial loss of system availability, etc.

Data: information in an oral, written, or electronic format that allows it to be retrieved or transmitted.

Disaster Recovery Plan: a crisis management master plan activated to recover IT systems in the event of a disruption or disaster. Once the situation is under control, a Business Continuity Plan should be activated.

Discovery: the first time at which an event is known, or by exercising reasonable diligence should have been known, by an officer, director, employee, agent, or agency contractor, including events reported by a third party to an agency or agency contractor.

Encryption: The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning. Applicable law may provide for a minimum standard for compliant encryption, such as HIPAA or NIST standards.

Eradication: the removal of a threat or damage to an information security system.

Event: an observable occurrence in a network or system.

Forensics: the practice of gathering, retaining, and analyzing information for investigative purposes in a manner that maintains the integrity of the information.

Hardware: the physical technology used to process, manage, store, transmit, receive, or deliver information. The term does not include software. Examples include laptops, desktops, tablets, smartphones, thumb drives, mobile storage devices, CD-ROMs, and access control devices.

Harm: although relative, the extent to which a privacy or security incident may actually cause damage to an agency or harm to an individual, reputation, financial harm, or results in medical identity theft.

Incident: an event which results in the successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system.

Incident Response Lead: person responsible for the overall information security Incident management within an agency and is responsible for coordinating the agency's resources which are utilized in the prevention of, preparation for, response to, or recovery from any Incident or Event.

Incident Response Team (IRT): led by the Incident Response Lead, the core team composed of subject-matter experts and information privacy and security staff that aids in protecting the privacy and security of information that is confidential by law and provides a central resource for an immediate, effective, and orderly response to Incidents at all levels of escalation.

Information Security: the *administrative, physical,* and *technical* protection and safeguarding of data (and the individual elements that comprise the data).

Integrity: The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity

Local Area Network (LAN): a private communications network owned and operated by a single organization within one location.

Malicious Code: a software program that appears to perform a useful or desirable function but actually gains unauthorized access to computer system resources or deceives a user into executing other malicious logic.

Malware: a generic term for different types of malicious code.

Penetration: gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Protected Health Information (PHI): information subject to HIPAA. Individually identifiable health information in any form that is created or received by a HIPAA Covered Entity, and relates to the individual's healthcare condition, provision of healthcare, or payment for the provision of healthcare as further described and defined in the HIPAA Privacy Regulations. PHI includes:

- demographic information unless such information is De-identified as defined in the HIPAA Privacy Regulations;
- "Electronic Protected Health Information" and unsecure PHI as defined in the HIPAA Privacy Regulations;
- the PHI of a deceased individual within 50 years of the date of death; and
- employment information.

Personal Identifying Information (PII): as defined by the Texas Business and Commerce Code §521.002(a)(1), "personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

- name, social security number, date of birth, or government-issued identification number;
- mother's maiden name;
- unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- unique electronic identification number, address, or routing code; and
- telecommunication access device as defined by the Penal Code §32.51.

Privacy: the right of individuals to keep information about themselves to themselves and away from others. For example, privacy in the healthcare context means the freedom and ability to share an individual's personal and health information in private.

Protocol: a set of formal rules describing how to transmit data, especially across a network.

Recovery: process of recreating files which have disappeared or become corrupted from backup copies.

Reportable Event: an event that involves a breach of Confidential Information requiring legal notification to individuals, government authorities, the media, or others.

Risk Assessment: the process by which the potential for harm is identified and the impact of the harm is determined. The process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Sensitive Data: while not necessarily protected by law from use or disclosure, data that is deemed to require some level of protection as determined by an individual agency's standards and risk management decisions. Some examples of “Sensitive Data” include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Internal communications
- Information determined to be authorized for use or disclosure only on a “need-to-know” basis

Sensitive Personal Information (SPI: as defined by the Texas Business and Commerce Code §521.002(a)(2) means:

1) An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and items are not encrypted:
    a. Social security number;
    b. Driver’s license number or government-issued identification number; or
    c. 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; or
2) Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or
    c. Payment for the provision of health care to the individual.

The term “Sensitive Personal Information” does not include publicly available information that is lawfully made available to the public from the federal, state, or local government.

Server: a processor computer that supplies a network of less powerful machines (such as desktop PCs and laptop computers) with applications, data, messaging, communication, information, etc.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

Vulnerability: weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

Wide Area Network (WAN): a communications network that extends beyond the organization’s immediate premises.

1.2 Common Acronyms

CDO: Chief Data Officer

CFAA: Computer Fraud and Abuse Act (1986)

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CJIS: Criminal Justice Information Services, a division of the FBI

CLIA: Clinical Laboratory Improvement Amendments

CPO: Chief Privacy Officer

CTO: Chief Technology Officer

FERPA: Family Educational Rights and Privacy Act (1974)

FISMA: Federal Information Security Management Act (2002)

FTI: Federal taxpayer information

HIPAA: Health Insurance Portability and Accountability Act (1996)

HITECH Act: Health Information Technology for Economic and Clinical Health Act (2009)

IRS: Internal Revenue Service

IRT: Incident Response Team

ISO: Information Security Office

IT: Information Technology

NIST: National Institute of Standards and Technology

PHI: Personal Health Information

PIA: Public Information Act, Government Code Ch. 552

PII: Personal Identifying Information

SPI: Sensitive Personal Information

SSA: Social Security Administration

TAC: Texas Administrative Code

SECTION 2

Incident Response Policy

Each agency should have a policy to address compliance with privacy and security breach management. Below is a sample policy which should be replaced by each agency and should be consistent with the agency's incident response plan.

2.1 Sample Security Incident Response Policy

Purpose

The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security Incidents in accordance with the Texas Administrative Code, Title 1, Chapter 202. This document sets forth the policy for incident management within the Agency.

Scope

This policy applies to and must be complied with by all Agency Users.

The User agrees to abide by this policy while employed or contracted with the Agency.

Roles and responsibilities of each function pertaining to the protection of Agency-owned systems and data are documented in Agency policy.

The User is responsible for understanding the terms and conditions of this policy.

Exemptions to this policy shall follow the process defined in Agency policy.

This policy is subject to change.

This policy applies to any computing device owned or leased by the Agency. It also applies to any computing device regardless of ownership, which either is used to store Agency-owned Confidential or Agency-sensitive data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure.

Policy

The Information Security Officer (ISO) is responsible for overseeing incident investigations in coordination with the Incident Response Team (IRT). The ISO shall recommend the IRT members to the Information Resources Manager (IRM) for approval. 1 TAC §202.26

The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security Incidents that fall under one or the following categories: 1 TAC §202.26

- Propagation to external systems
- Violation of applicable federal and/or state laws which will require involvement from law enforcement

- Potential modification or disclosure of Confidential Information as defined in the Agency Data Classification Policy.

	The Agency shall notify appropriate individuals (which must include the State CISO and the State Cybersecurity Coordinator) within 48 hours if it is believed that personal information owned by the Agency has been used or disclosed by or for unauthorized persons or purposes.	TGC §2054.1125, TBC §521.053
	The ISO shall establish an Incident Criticality matrix. This matrix will define each level of escalation, detail the appropriate response for various incidents, and establish the appropriate team participants.	1 TAC §§202.21-22
	The ISO shall establish and document appropriate procedures, standards, and guidelines regarding Incidents.	1 TAC §202.21
	The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation. Any electronic device containing data owned by the Agency may be subject to seizure and retention by the ISO.	
	The Chief Information Security Officer, Chief Privacy Officer, or Agency General Counsel (as appropriate) will work directly with law enforcement regarding any Incidents that may have violated federal or state laws. If an Incident is determined to be the result of a privacy violation by a User, the ISO shall notify the User's supervisor and Human Resources of the violation(s), or the Inspector General's Office, as applicable, for appropriate action.	
	The ISO shall provide a summary report for each valid Security Incident to the IRM within five business days after the incident has been closed.	
Disciplinary Action	Management reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts the normal operation of agency information systems or violates state or federal law.	
	Any User who has violated this policy may be subject to disciplinary action, up to and including termination of employment or contract with DIR.	
	The Agency will cooperate with appropriate law enforcement if any User may have violated federal or state law.	
Document Change Management	All changes to this document shall follow the process defined in Agency policy.	
	The ISO will be responsible for communicating the approved changes to the organization.	1 TAC § 202.21

SECTION 3

Privacy/Security Event Initial Triage Checklist

1) **Incident Response Team:** Assemble Incident Response Team (IRT) in response to an actual or suspect event/incident. Meet daily if necessary, with priority over other work, possibly requiring after-hours activities.

2) **Secure data:** Secure data and confidential information and limit immediate consequences of the event. Suspend access and secure/image assets as appropriate, e.g. harden or disable system or contact internet search engines if appropriate to clear internet cache.

3) **Data elements:** Determine the types, owners, and amounts of confidential information that were possibly compromised.

4) **Data source:** Identify each location where confidential information may have been compromised and the business owner of the confidential information.

5) **Scope and escalation:** Confirm the level and degree of unauthorized use or disclosure (includes access) by the named or unidentified individuals or threats.

6) **Number of individuals impacted:** Determine the number of individuals impacted. The number may implicate breach notification requirements, e.g. individual or media notice.

7) **Discovery date:** Determine the date the agency or contractor knew or should have known about the event/incident.

8) **Management alert:** Advise appropriate internal management.

9) **External communications, as required:** Advise external contacts, such as DIR, legislative leadership, the Office of the Inspector General, the Office of the Attorney General, Secretary of State (SOS) (if election data involved), law enforcement, outside counsel, and applicable regulatory authorities.

10) **Investigate:**

    a. Interview: Identify and interview personnel with relevant knowledge, e.g., determine whether and by whom access may have been approved, who discovered the risk, etc.

    b. Documents: Gather and review contracts and provisioning documents (documents authorizing access or restricting use or disclosure).

    c. Root Cause Analysis: Prepare RCA which describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence.

    d. Event and Threat Impact Analysis (see section on Event Threat and Impact Analysis below).

11) **Mitigation:** Revise policies, process, or business requirements, sanction workforce, enforce contracts, etc. to reduce the likelihood of event reoccurrence. Set timeline and assign responsibility to ensure accountability. Follow-up to ensure corrective action initiated and completed on time or decision to accept the risk of reoccurrence, and report appropriately.

SECTION 4

Event Threat, Impact Analysis, and Escalation Criteria

The investigation of the incident/event should include an Event Threat and Impact Analysis to accurately categorize the impact of the event on the organization. Once the event's impact level is understood it may be appropriate to escalate the incident response and contact other entities.

4.1 Event Threat and Impact Analysis

The National Institute of Standards and Technology (NIST) Special Publication NIST 800-61, Computer Security Incident Handling Guide, provides advisement on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media. Per NIST 800-61, section 3.2.6 (Incident Prioritization) relevant factors for event threat and impact/escalation criteria include:

- **Functional Impact.** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems.
- **Information Impact.** Incidents may affect the confidentiality, integrity, and availability of the organization's information.
- **Recoverability.** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.

While there is no single model for determining event impact, the below tables provide guidance on defining impact to organization systems, organization information (business impact), and organization ability to recover from an event (possible responses). Organizations should consider each category to assure proper response and recovery from these events.

Table 4.1: Examples of functional impact categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users.
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users.

Table 4.2: Examples of possible information impact categories

Category	Definition
None	No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes.
Integrity Loss	Sensitive or proprietary information was changed or deleted accidentally or intentionally.

Table 4.3: Examples of recoverability effort categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation.

4.2 Event Escalation: Communication

NIST 800-61 Computer Security Incident Handling Guide provides advisement on escalation of security incidents. Section NIST 800-61, 3.2.7 (Incident Notification) outlines important contacts and modes of communications.

Key Contacts. Organizations should establish an escalation process for instances when key individuals outside of normal technical response processes must be notified. Among those to be considered are:

- CIO or Information Resources Manager (IRM)
- CISO or Information Security Officer (ISO)
- CPO or Privacy Officer
- Other incident response teams within the organization
- External (contractor) incident response teams, if appropriate
- System owner
- Human resources
- Public affairs
- Legal department
- US-CERT (required for systems operated on behalf of the federal government)

- Law enforcement, if appropriate
- Federal government agencies, if appropriate
- Department of Information Resources Office of the CISO (Mandated for Texas Agencies)

Contact Methods. Organizations may need to provide status updates to certain external and internal parties. Among communication methods to be considered are:

- Email
- Website (internal, external, or portal)
    - Note: The official State Portal to notify DIR is SPECTRIM and all ISOs have access to this system
- Telephone calls
- In person (e.g., daily briefings)
- Voice mailbox greetings (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status; use the help desk's voice mail greeting)
- Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)

SECTION 5

Breach Notice Criteria

Certain types of breaches carry legal notification responsibilities. This section includes information about breach notification statutes and rules according to Texas law, federal laws and regulations, and other states' laws. ***NOTE*** As of 9/1/2017 TGC §2054.1125 requires notification of the Texas Office of the Chief Information Security Officer and the State Cybersecurity Coordinator within 48 hours of discovery for all Breaches (actual or suspected) which require disclosure by law or agreement. For any Breach involving Election Data, the Office of the Secretary of State must be notified.

Table 5.1: Texas legal requirements for breach notices

Breach Notice	Citation	Requirement	Notes
Texas Identity Theft Enforcement and Protection Act (2005) Updated 2019	Texas Business and Commerce Code Ch. 521, §521.053	Report any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person or to the data owner immediately. Public reports may be required for breaches involving 10,000 or more individuals. An organization that is required to disclose or provide notification under this section, is required to notify the Texas Attorney General if the breach involves at least 250 Texas residents. This notification must include: 1. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach; 2. The number of residents of this state affected by the breach at the time of notification; 3. The measures taken by the person regarding the breach; 4. Any measures the person intends to take regarding the breach after the notification under this subsection; and 5. Information regarding whether law enforcement is engaged in investigating the breach.	Government Code §2054.1125 makes Business and Commerce Code §521.053 applicable to state agencies.

Table 5.2: Federal legal requirements for breach notices

Breach Notice	Citation	Requirement	Notes
HIPAA	45 CFR §164.404	Notify individual or Covered Entity of a breach of unsecured protected health information which poses a significant risk of financial, reputational, or other harm to the individual. Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach.	Applies only to HIPAA Covered Entities and HIPAA-protected health information. A Business Associate of a Covered Entity is required to notify the Covered Entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice.
Federal Financial Participation	CMS SMDL #06-022	CMS-regulated entities must notify CMS within one clock hour according to Sep. 2006 CMS letter to State Medicaid Directors	Unclear if HIPAA HITECH eliminated the CMS requirement. SNAP, TANF, and CHIP each have similar authorizations to use or disclose Medicaid information that identifies an applicant or

			recipient is limited to use or disclosure "directly in connection with program administration," but have no breach notice requirement.
Internal Revenue Service	By data sharing agreement with the IRS, pursuant to IRS Publication 1075 §10	Notify TIGTA and IRS Office of Safeguards of compromised IRS or SSA data within one clock hour from discovery of an actual or suspected breach. Follow individual agency procedures for notifying impacted individuals.	The IRS Office of Safeguards may require individual notification.
Social Security Administration (SSA)	By contract between SSA and Agency which defers to IRS Publication 1075	Notice required to SSA within one clock hour of discovery. Follow instructions of SSA to notify impacted individuals, if any.	SSA may require individual notification.
Federal Trade Commission (FTC)	Health Breach Notification (PHR, EHR Vendors) 16 CFR Part 318	Requires a vendor of personal health records to notify the individual US Citizen and the FTC following the discovery of a breach of security of unsecured PHR-identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR-related entity.	Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third-party service providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. "Breach" is acquisition unauthorized by the individual. Notify without unreasonable delay and in no case later than 60 calendar days after the breach discovery.
Family Educational Rights and Privacy Act (1974)	20 USC §1232g, 34 CFR Part 99	None. FERPA guidance recommends having breach response plans.	Applies to educational institutions regarding the privacy of personally identifiable information contained in education records of students. Consent is generally required to disclose education records.

State Data Breach Notification Laws: The National Conference of State Legislatures maintains a matrix of state data breach laws. As of April 2019, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

Table 5.3: Security breach notification statute in other states, Texas, and territories (NCSL)

State	Citation
Alabama	2018 S.B. 318, Act No. 396
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-545
Arkansas	Ark. Code § 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.82 & Cal. Civ. Code §§ 1798.100 - 1798.199
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-439 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 *et seq.*
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. § 51:3071 *et seq.*
Maine	Me. Rev. Stat. tit. 10 § 1346 *et seq.*
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 252E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 356-C:19, -C:20, -C:21
New Jersey	N.J. Stat. § 56:8-163
New Mexico	N.M. 2017 H.B. 15, Chap. 36
New York	N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat. §§ 75-61, 75-65
North Dakota	N.D. Cent. Code § 51-30-01 *et seq.*
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166

Oregon	Oregon Rev. Stat § 646A.600 *et seq.*
Pennsylvania	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	R.I. Gen. Laws § 11-49.3-1 *et seq.*
South Carolina	S.C. Code § 39-1-90
South Dakota	S.D. Cod. Laws §§ 20-40-20 to -46 (2018 S.B. 62)
Tennessee	Tenn. Code § 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053, Tex. Ed. Code § 37.007(b)(5)
Utah	Utah Code §§ 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9 § 2430, 2435
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05
Washington	Wash. Rev. Code § 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 *et seq.*
Wisconsin	Wis. Stat § 134-98
Wyoming	Wyo. Stat. § 40-12-501 *et seq.*
District of Columbia	D.C. Code § 28-3850 *et seq.*
Guam	9 GCA § 48-10 *et seq.*
Puerto Rico	10 Laws of Puerto Rico § 4051 *et seq.*
Virgin Islands	V.I. Code tit. 14 § 2208

SECTION 6

Post-Incident Checklist

The Computer Security Incident Handling Guide (NIST 800-61) provides advisement on event analysis activities. Per section 3.4.1 (Lessons Learned) and section 3.4.2 (Using Collected Incident Data) relevant factors for post-incident and root cause analysis include:

1) **Learning and improving.** Incident Response Teams should hold "lessons learned" meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:
    a. Exactly what happened, and at what times?
    b. How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
    c. What information was needed sooner?
    d. Were any steps or actions taken that might have inhibited the recovery?
    e. What would/should staff and management do differently the next time a similar incident occurs?
    f. How could information sharing with other organizations have been improved?
    g. What corrective actions can prevent similar incidents in the future?
    h. What precursors or indicators should be watched for in the future to detect similar incidents?
    i. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

2) **Follow-up reporting.** An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
    a. Creating a formal event chronology (including time-stamped information from systems);
    b. Compiling a monetary estimate of the amount of damage the incident caused;
    c. Retaining follow-up reports as specified in retention policies.

3) **Data collected.** Organizations collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event.

4) **Root Cause Analysis.** Organizations performing root cause analysis should focus on relevant objective assessment activities including:
    a. Reviewing of logs, forms, reports, and other incident documentation;
    b. Identifying recorded precursors and indicators;
    c. Determining if the incident caused damage before it was detected;
    d. Determining if the actual cause of the incident was identified;
    e. Determining if the incident is a recurrence of a previous incident;
    f. Calculating the estimated monetary damage from the incident;
    g. Measuring the difference between initial impact assessment and the final impact assessment; and
    h. Identifying measures, if any, that could have prevented the incident.

SECTION 7

Incident Response Team Templates

Included in this section are templates relevant to the operation of an Incident Response Team: the title and contact page for the plan's sponsor/owner, a sample charter, a membership list that lists important roles, an example record of meeting minutes, a post-meeting action list, and a list of important state government contact information. The plan sponsor or owner is responsible for modifying these templates for the incident response team's purposes. Brackets indicate where the IR Lead should customize to reflect the agency.

7.1 Title and Contact Information for Plan Sponsor/Owner

[Agency Name]

Information Privacy or Security Incident Response Team Redbook

For questions or further information, please contact:

	Name	Phone	Email
Sponsor			
Owner			

"Sponsor" is the executive responsible for compliance
"Owner" is the owner of this document

7.2 IRT Charter

Information Privacy or Security Incident Response Team Charter

Charter Purpose:

This Incident Response Team (the "IRT") Charter establishes membership, subject matter experts, roles, responsibilities, and activities of the [agency] IRT to respond to an actual or suspected information privacy or security event/incident.

IRT Mission:

The IRT mission is, first, to prevent incidents by reasonably anticipating, detecting, and planning for actual and suspected privacy or security events; and second, to respond to and mitigate privacy or security events.

Overview:

The Incident Response Team (the "IRT") is a standing team of internal personnel established by [Executive Management] in this [Charter] with expertise in responding to a significant actual or suspected privacy or security event or incident. The IRT operates on behalf of [Executive Management] and engages, informs, and receives support from [Executive Management]. There [is/is not] a set protocol to initiate the IRT activities in response to an actual or suspected event/incident. Once activated, the IRT has authority to [request cooperation/establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours].

Responsibilities and Roles:

<u>Responsibilities:</u>

1) **Anticipate and prepare** [the agency] for privacy or security events/incidents which can be reasonably anticipated;
2) **Respond** to actual or suspected events/incidents on behalf of [the agency] as needed, with activities such as:
    a. Triage (see section 2);
    b. Communication, internal and external, as needed according to [agency's] communications protocol (e.g. funneled to the top from a deputy, for example) (see communications templates)
    c. Track and document IRT activities and discoveries; and
    d. Prepare post-event/incident analysis and lessons learned.

Examples of significant events/incidents within IRT responsibility:

- Uncontained or escalating malware attack on system (computer virus, worm, bot, or Trojan);
- Abuse, theft, misuse, or loss of data or hardware (including unauthorized use, disclosure, or access to computer accounts, systems, or data; hacking; human error);

- Improper use or disclosure of information or information resources as outlined in [agency] standards or contracts including e-mail, equipment, Internet, and acceptable data use (includes human resources or contractor misuse or error);
- Many individuals or a large amount of sensitive data impacted; or
- Events likely to be high-profile or create a significant risk of individual harm (e.g., risk of financial harm, reputational harm, or medical identity theft).

Roles:

1) **The IRT Lead.** The Lead of the IRT may:
    a. Be designated by and reporting to [Executive management]. The IRT is led by [____________] or his or her designee.
    b. Declare an incident
    c. Establish, maintain, and update written IRT protocols or incident response plans
    d. Identify roles and responsibilities for IRT standing members
    e. Request or designate ad hoc members for particular events as needed
    f. [request cooperation / establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours]

2) **IRT Standing Members.** The standing members include named individuals or representatives.

3) **Ad hoc Members or Subject Matter Experts.** Ad hoc members or Subject Matter Experts may be designated as ad hoc resources by the IRT Lead.

7.3 IRT Membership by Roles

The following table contains contact information for current IRT members. Please note that, in some cases, a member listed below may have designated another agency employee to represent him or her. Also, while the IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.

Standing IRT Membership Contact Information - *<u>Confidential</u>*

Standing Members	Name	Phone	Email	After-hours contact
IRT Lead				
[Chief Information Officer or designee]				
[Chief Information Security Officer or designee]				
[Information Resources Manager or designee]				
[Internal Audit]				
[Office of Inspector General]				
[Other]				
[Other]				
[Other]				
Legal Counsel to the IRT – to avoid losing attorney-client privilege, *do not list legal as a member*				

Ad Hoc IRT Members

Ad hoc Members	Name	Phone	Email	After-hours contact
[Relevant business area, department, division]				
[Communications]				
[External Relations]				
[Open Records]				
[Third parties, e.g., contractor]				
[Department of Information Resources designee]				

[Counsel, Office of Attorney General]				
[Vendor for Breach Management services]				
[Law Enforcement]				
[Outside legal counsel]				
[Other]				
[Other]				
[Other]				

Note 1: Standing members are relatively static; ad hoc members are designated for each incident.
Note 2: After hours contact information is critical to incident handling.

7.4 IRT Meeting Minutes

CONFIDENTIAL

Meeting Minutes for [Agency] IRT Meeting____, 20__

Purpose: The purpose of this message is to provide updates regarding the IRT activities in response to confirmed privacy and/or security incidents involving personal or confidential information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action. This Alert will be regularly updated as more information becomes available.

Summary
Brief incident summary:
Participants
IRT Members Present: *IRT Members Not in Attendance:* *Guests:*
Current Updates
1. 2. 3.
Prior Updates
1. 2. 3.
Next Steps
1. 2.
Next Scheduled Meeting

__:00, _. m.,____.____, 20___
Location:
Conference No.:______________________Access Code: ________________________

7.5 IRT Action List

IRT: Identification Name or Number

Action Items Status

Current Updates as of____. __,20__

Item	Date	Action	Assigned To	Status
1.				
2.				
3.				
4.				
5.				
6.				

7.6 IRT State Government Contact Information

IRT State Government Contact Information

Entity	Contact	Division/Location	Email/Office Telephone
Office of the Governor			
Lieutenant Governor			
Speaker of the House			
State of TX Office of the Chief Information Security Officer			
State Cybersecurity Coordinator			
[Agency Board or Commission Chair]			
[Agency Oversight Senate Committee Chair]			
[Agency Oversight House Committee Chair]			

SECTION 8

Additional Templates

Included in this section are additional guidelines and templates which may be of use to the Incident Response Team: the Identity Theft Protection Criteria, a sample Internal Management Alert, a sample Notice to Individuals Affected by Incident, and a Public (Media) Notice. The plan sponsor or owner is responsible for modifying these templates to fit the IRT's purpose. Brackets indicate where the IR Lead should customize the template to reflect the agency's needs.

8.1 Identity Theft Protection Criteria

Although it is optional for a state agency to provide identity theft protection, each agency should evaluate the risk of financial or medical identity theft occurring. If the risk is deemed significant, the agency may consider this type of protection. In addition to deciding whether to provide the protection, an agency should consider an appropriate length of time to provide the protection. Ultimately the decision to provide protection should be made at an Executive-level position. Should an agency determine identity theft protection is appropriate, there are various types and level of protection to choose from on the market, including:

- Identity theft insurance with various coverages or guarantees
- Credit report monitoring
- Claims monitoring
- Monitoring of websites used to trade stolen information
- Theft assistance resolution

DIR has contracts with one or more vendors of identity theft amelioration services. As noted, commercial identity theft protection varies in the means and extent of coverage. While some carriers offer compensation for expenses incurred as a result of theft, others simply provide credit monitoring and alerts to an individual in the event of credit activity. In addition to assistance for affected individuals, breach management services can be procured to assist an entity responsible for a breach, as well as provide risk assessment, mitigation, or remediation services. As circumstances warrant, [Agency] may elect to procure commercially available identity theft protection or breach management services, especially for high-profile events likely to lead to significant harm to impacted individuals or reputational harm or cost to [Agency].

[Agency] will consider the following criteria to determine whether to procure identity theft protection or breach management services:

1) Contract opportunities made available to state agencies by the Department of Information Resources for identity theft or breach management services [see resources page].
2) Contractual requirements imposed upon the [Agency] vendor or contractor, or other third party responsible for the breach, to provide identity theft protection, breach management services to the agency, or any other indemnification or hold harmless contract provisions.
3) Degree and scope of the breach and the degree or type of risks to individuals, such as financial, reputational, or other harm (such as medical identity theft or criminal identity theft), dependent upon the various forms of identity theft.
4) The extent to which commercial services will be unable to detect or deter harm such as medical or criminal identity theft for the breach at issue.
5) No or low-cost measures available to impacted individuals to protect themselves, such as a self-imposed credit fraud alert, a credit freeze request to one of the credit bureaus [see breach notice template for more information], or filing a police report. Some options for impacted individuals include:
    a. A **fraud alert** which can help prevent an identity thief from opening additional accounts in a consumer’s name in 90 days.

    b. A **security freeze**, also known as a **credit freeze**, which is a warning sign to businesses or others who may use an individual's credit file and requires a police report.
    c. Contacting the **Consumer Protection Division** of the Texas Office of the Attorney General.
6) The ability to link the breach event to an identity theft event or other harm.
7) The cost to the agency or agency contractor for the provision of identity theft or breach management services.

8.2 Internal Management Alert Template

NOTICE: The information contained in this message and any attachment to this message are confidential under state or federal law and may be protected by attorney-client privilege. If you have received this message in error, please immediately notify the sender of this e-mail, then delete or destroy it and any attachment(s). Thank you.

Agency Data Security Incident Alert

Purpose: The purpose of this message is to inform you of a suspected or confirmed privacy and/or security incident involving personal information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action and will be regularly updated as more information becomes available.

Summary
Brief incident summary:
Immediate Recommendations:
1. 2. 3.
Next Steps:
1. 2. 3.
Next Scheduled Update:
[Time/Day/Date or "As conditions warrant"]

8.3 Notice to Individuals Affected by Incident

<Date>

<<Title>> <<First Name>> <<Last Name>>

<<Address>>

<<City>>, TX. <<Zip>>

Dear <<Title>> <<Last Name>>:

Your name and certain personal information was [exposure type/description]. This means that information may have been exposed without your authorization or the authorization of [Agency]. We apologize for any inconvenience this offers you. [Although there is no evidence that any information has been misused, the state is providing you with free credit monitoring coverage.]

[Describe the incident and what the agency is doing to mitigate the incident.]

We are committed to helping you safeguard your information. [[Agency] is providing you with free credit monitoring and identity theft services for one year. This service includes an insurance policy of up to $[_] in identity theft coverage, a year of [name of Agency's contracted Breach Management Vendor product] coverage, and a full-service identity restoration team to guide you through the recovery process if anyone tries to misuse your information. You must enroll to take advantage of this free service.]

We have set up a website that will help you protect your information and will provide you with updates on this matter. You may also call [name of Agency's contracted Breach Management Vendor] to ask for help in keeping your data safe. **If you are enrolling a minor child, you will need to call [Breach Management Vendor] to process their enrollment manually. Child enrollment cannot be conducted online.**

We recommend that you also take the following steps to protect your identity:

- Contact one of the national credit reporting agencies below and ask for a fraud alert on your credit report. The agency will alert all other agencies. Remember to renew these fraud alerts every 90 days. The state does not have authority to do this for you, as the credit bureaus must have your permission to set up the alerts.
- The credit reporting agencies do not knowingly maintain credit files on children under the age of 18. You may contact each agency to determine if a child has a file or if the child's information has been misused:

Equifax
P.O. Box 740241 — www.fraudalerts.equifax.com
Atlanta, GA 30374 — Fraud Hotline (toll-free): 1-877-478-7625

Experian
P.O. Box 2002 — www.experian.com
Allen, TX 75013 — Fraud Hotline (toll-free): 1-888-397-3742

TransUnion
P.O. Box 6790 — www.transunion.com
Fullerton, CA 92834 — Fraud Hotline (toll-free): 1-800-680-7289
Report fraud: fvad@transunion.com

- Request a copy of your credit report from the credit reporting agencies and carefully review the reports for any activity that looks suspicious.

- Monitor your [bank account activity / health care records / medical insurance company explanation of benefits] to ensure there are no transactions or other activity that you did not initiate or authorize. Report any suspicious activity in your records to your [bank / health care provider / health insurance company's privacy officer].

- Report any suspicious activities on your [credit reports or bank account / health care or health insurance records] to your local police or sheriff's office and file a police report. Keep a copy of this police report in case you need it to clear your personal records.

- Learn about the Federal Trade Commission's identity theft programs by visiting www.ftc.gov/bcp/edu/microsites/idtheft or by contacting the Federal Trade Commission's toll-free Identity Theft helpline at 1-877-ID-THEFT (1-877-438-4339); TTY:1-866-653-4261.

- [Enroll in free credit monitoring and identity theft services provided by the state. There is no cost to you for the service, but **you must enroll**. You can enroll online at__________or by contacting [Agency's contracted Breach Management Vendor's] Customer Care Center toll-free at_______________.]

- **[To enroll your minor child, please call [Agency's contracted Breach Management Vendor's] Customer Care Center at__________to manually enroll them. Child enrollments cannot be conducted online.]**

- Monitor the website at [Agency's contracted Breach Management Vendor's agency / Agency's own site] for periodic updates.

[Agency] regrets that this action is necessary. Please be assured that we are committed to helping you protect your credit and identity and in ensuring that your information is safe and secure.

If you have any questions, please call [Agency contact] at________or contact by email at ________.

Sincerely,

[Authorized signatory]

8.4 Public (Media) Notice

In the event that you choose to notify the public at large, the information in your notice should mirror the information contained in the breach notice to individuals affected (section 7.3). Media notice may be legally required; please see Breach Notice Criteria. A media notice should be developed through your usual public communication processes and contain the following information:

- Brief description of the details of the event
- Description of the individuals affected in the aggregate
- Description of actions taken by the agency
- Statement as to whether evidence indicates the data may have been misused
- Contact information for questions

8.5 Post-Mortem and Improvement Plan

INCIDENT POST-MORTEM

Cyber Incident	[Use your organization's naming convention of the incident.]
Dates and Times	[Indicate at a minimum the start/end dates/times of the incident. Include a full incident chronology if available.]
Description	[Give a brief description of the incident.]
Impact	[What was the impact to the organization?]
Detection	[How was the incident detected?]

Learning and Improving

Question	Response	Comment
How well did the staff and management perform?	.	.
Were documented policy and procedures followed?	.	.
Were the procedures adequate?	.	.
Was the actual cause identified?	.	.
What information was needed sooner?	.	.
Were any steps taken that might have inhibited recovery?	.	.
What should/would staff/management do differently the next time a similar incident happens?	.	.
How could information sharing (in/out) with other organizations have been improved?	.	.
What corrective actions can prevent or lower the likelihood of similar incidents in the future?	.	.
What precursors or indicators of compromise should be watched in the	.	.

	future to speed up detection?		
	What additional tools and/or resources are needed to address future incidents?	.	.
	What tools, processes, metrics or resources could be in place and/or monitored to detect a similar incident sooner?	.	.

	Question	**Response**	**Comment**
Root Cause Analysis	What could have prevented the incident?	.	.
	Was there damage caused prior to detection?	.	.
	Is the incident a recurrence of a previous incident?	.	.
	Was the actual cause identified?	.	.
	Was there a difference between initial impact assessment and the final impact assessment?	.	.
	Were there any leading-edge indicators of detection that were missed?	.	.

Metrics	[Enter any related metrics e.g., mean-time-to-incident-discovery, cost of recovery, time from detection to containment, …]
Approximate cost of the incident	[What was the cost in time, materials, human resources, and lost productivity to the organization in dollar figures? These could range from time and resources, equipment replacement costs, agency downtime, idle employee time, backlog catchup overtime, etc.]

IMPROVEMENT PLAN

This improvement plan has been developed specifically for [Organization] as a result of the Cyber Incident that occurred on [date].

Issue/Area for Improvement	Corrective Action	Primary Responsible	Start Date	Completion Date
1. [Area for Improvement]	[Corrective Action 1]			
	[Corrective Action 2]			
	[Corrective Action 3]			
2. [Area for Improvement]	[Corrective Action 1]			
	[Corrective Action 2]			

SECTION 9

External Contacts

External Partners. Collaboration with external entities may be necessary to assist with incident response or for auxiliary support. The IRT shall ensure that all those participating in the incident response work together efficiently and effectively.

The tables below identify contact information of external partners with whom the agency may need to collaborate in the event of an Incident as well as resource pages and other useful information.

Table 9.1: State of Texas Contacts

Resource	Services	Contact Information
Austin Police Department Digital Analysis Response Team (DART)	Conducts investigations of technology-related crimes in the City of Austin and helps other law enforcement agencies perform forensic examinations of digital evidence.	Contact number: (512) 974-8631
Office of the Attorney General	The agency of the state's chief law enforcement official.	OAG main number: (512) 463-2191 Deputy Attorney General for Defense Litigation: (512) 463-0150 State Law Enforcement Criminal Investigation: (512) 936-2777 Contact OAG Information Security Officer (for Incidents affecting OAG data system or staff). Identity Theft Legal Resources and Alerts: https://www.oag.state.tx.us/consumer/index.shtml
Office of the Attorney General, Criminal Investigations Division	Investigates cybercrime and provides computer forensics services to locate and preserve digital evidence.	Criminal Investigations: CJID@oag.state.tx.us (512) 475-4220 Cybercrimes: (512) 463-9570

State Auditor's Office, Special Investigations Unit	Investigates criminal offenses affecting state resources, including computer security breaches.	Hotline: 1-800-892-8348
Texas Facilities Commission	Provides facilities services (including emergency management) for state buildings and leasing services to state agencies.	24-hour Facilities Management: (512-) 463-3600 State Leasing Services: leasing@tfc.state.tx.us (512) 463-3331
Texas Department of Information Resources, Security Operations Center	Provides information security services and communications technology services, including Incident response and assistance, to Texas state agencies, local governments, public education entities, and special districts.	DIR Network Security Operations Center: Security-alerts@dir.texas.gov 888-839-6762 Option 1 network Option 2 Security
Texas Department of Public Safety, Emergency Management Division	Coordinates the state emergency management program and manages the Statewide Operations Center (SOC), which monitors threats, makes notification of threats, and provides information on emergency incidents to local, state, and federal officials.	Division of Emergency Management Headquarters: (512) 424-2138 SOC: soc@dps.texas.gov Operations Officers: (512) 424-2208 (512) 424-2277
Texas Rangers, Texas Department of Public Safety	Leads criminal investigative responsibility for major Incident crime investigations.	Austin Headquarters: (512) 424-2160 rangers@dps.texas.gov

Table 9.2: Federal Contacts

Resource	Services	Contact Information
Federal Bureau of Investigation	Cyber squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information.	Texas Field Offices: Dallas: (972) 559-5000 El Paso: (915) 832-5000 Houston: (713) 693-5000 San Antonio: (210) 225-6741
Federal Emergency Management Agency (FEMA)	Provides disaster response and recovery assistance.	1-800-621-FEMA (3362)
National Cyber Security Division (NCSD), US Dept. of Homeland Security	Works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.	Response coordination: (202) 282-8000

CERT Coordination Center (CERT/CC)	Federally-funded CERT provide technical advice to federal, state, and local agencies on responses to security compromises.	CERT 24-hour hotline: (412) 268-7090 forensics@cert.org
US Secret Service	Investigates financial crimes, including identity theft.	Austin Field Office: (512) 916-5103
US Treasury Inspector General for Tax Administration (TIGTA) and Office of Safeguards	Works with agencies to ensure that all appropriate actions are taken with regard to Federal Tax Information.	TIGTA Field Division, Dallas: (972) 308-1400
Federal Trade Commission (FTC)	Regulates consumer business practices.	http://www.ftc.gov Detecting identity theft: http://www.ftc.gov/idtheft
National Institute of Standards and Technology (NIST), US Dept. of Commerce	Advances US measurement science, standards, and technology, including accelerating the development of and deployment of standards and systems that are reliable, usable, interoperable, and secure. Assigned certain information security responsibility under the Federal Information Security Management Act of 2002 (FISMA, 44 USC § 3541, *et seq.*). NIST has published over 200 information security documents on information security standards, guidelines, and other resources necessary to support the federal government.	Main office: (301) 975-NIST inquiries@NIST.gov http://www.nist.gov/index.html Publications: http://csrc.nist.gov/publications/
Office for Civil Rights (OCR), US Dept. of Health and Human Services	Oversees federal civil rights and health information privacy, security, and breach notice by HIPAA.	http://www.hhs.gov/ocr/office/index.html
US Postal Service Inspector Service	The law enforcement arm of the US Postal Service, which investigates crimes that may adversely affect or fraudulently use the US Mail, the postal system, or postal employees.	https://postalinspectors.uspis.gov

Table 9.3: Industry Contacts

Resource	Services	Contact Information
Ponemon Institute	Conducts independent research on privacy, data protection, and information security policy.	http://www.ponemon.org/index.php

Credit Bureaus	Collects reported consumer credit for purposes of credit risk assessment and scoring or other lawful purposes. Consumers may request a 90-day or 7-year fraud alerts be attached to their credit bureau files by contacting one credit bureau which will in turn notify other bureaus. A credit freeze must be requested from each bureau.	Equifax: P.O. Box 740241 Atlanta, GA 30374 Fraud Hotline (toll-free): 1-877-478-7625 www.fraudalerts.equifax.com Experian P.O. Box 2002 Allen, TX 75013 Fraud Hotline (toll-free): 1-888-397-3742 www.experian.com TransUnion P.O. Box 6790 Fullerton, CA 92834 Fraud Hotline (toll-free): 1-800-680-7289 www.transunion.com Email to report suspected fraud: fvad@transunion.com Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281 1-877-322-8228 http://www.ftc.gov/freereports www.AnnualCreditReport.com
American Health Information Management Association (AHIMA)	AHIMA is an association of health information management professionals with a useful resources page for health data.	http://www.ahima.org/resources/infocenter/psc.aspx
Health Information Management Systems Society (HIMSS)	HIMSS is an association of health information management professionals with resources page for health data.	http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266
Payment Card Industry – Data Security Standards (PCI-DSS)	Payment card data security standards set by the payment card industry.	https://www.pcisecuritystandards.org/security_standards/

Table 9.4: Press Contacts

Resource	Services	Contact Information
Texas Press Contacts	Texas Media Directory (subscription for distribution lists for other cities and counties).	http://www.texasmedia.com

SECTION 10

Legal References

This section covers a list of federal and state laws establishing relevant standards for types of confidential data, including a brief summary and a citation. The list is not comprehensive; please refer to legal counsel for other relevant laws.

10.1 Texas Laws and Regulations for Data Privacy and Security

Texas Public Information Act	The Public Information Act contains provisions pertaining to information disclosure:	
	The agency may not withhold information, even confidential information, if requested by a legislator or the Legislature for legislative purposes.	TGC § 552.008
	Information confidential by law is excepted from disclosure. Example: TGC § 2059.055.	TGC § 552.101
	Is this IRT Redbook subject to disclosure under the Public Information Act? Some possible exceptions to disclosure for all or part of the book:	
	Employee home addresses, home phone numbers, social security numbers, and family information is exempted from disclosure if the employee did not choose to disclose under §522.024, which may apply to IRT contact information.	TGC § 552.117
	Note: employee home email addresses possibly also excepted under 552.117. Unresolved issue: disclosure of employee work email address (otherwise public) may reveal who is on IRT.	
	Network security is exempted from the requirement to disclose in the Public Information Act.	TGC § 552.139, TGC § 2054.055, ORD 581 (1990)
	Are records relating to the breach itself and the agency's response confidential? Possible exceptions to disclosure include:	
	Some personnel information may be private if in the personnel file; some transcripts are exempt from disclosure.	TGC § 552.102, TGC § 552.024, TGC § 552.117
	Information related to litigation, if pending or reasonably anticipated, is exempt from disclosure.	TGC § 552.103
	Information related to competition or bidding, generally while bidding is in process, is exempt from disclosure.	TGC § 552.104, TGC § 552.128

	Information submitted by a potential vendor or contractor is also exempted from disclosure.	
	Attorney-client privilege and court-ordered confidentiality can be used to keep certain information from disclosure, with some limitations (see TGC § 552.022(b)).	TGC § 552.107, TGC § 552.022(b)
	Certain law enforcement records may be kept private, generally while the case is pending.	TGC § 552.108
	Trade secrets are exempt from public disclosure.	TGC § 552.110
	Agency memoranda which would not be made available to a party in litigation (including attorney work product) are exempt from disclosure.	TGC § 552.111
	Credit and debit card numbers as well as access device numbers may be kept from disclosure; additionally according to ORD 684 (2009), insurance policy numbers, bank account numbers, and bank routing numbers can also be withheld from disclosure.	TGC § 552.136, ORD 684 (2009)
	Email addresses of the public are exempt from disclosure.	TGC § 552.137
	Social security numbers are exempt from disclosure.	TGC § 552.147
	Note: the information that was the subject of the breach is also presumed to be protected from disclosure, possibly under sections not cited above. Each agency should be aware of how its own information is protected under the Public Information Act.	
	With a few exceptions, agencies must receive a decision from the Office of the Attorney General before it can withhold information from a PIA request. The PIA contains some pitfalls, including some very strict deadlines. All agencies should consult an attorney or PIA coordinator for further guidance.	
Privacy Policy Necessary to Require Disclosure of SSN	A person may not require an individual to disclose one's social security number to obtain goods or services from or enter into a business transaction with the person unless the person adopts a privacy policy, makes the policy available to the individual, and maintains the confidentiality and security of the social security number. The statute also prescribes required elements of a privacy policy.	BCC § 501.052
Texas Identity Theft Enforcement and Protection Act	The Texas Identity Theft Enforcement and Protection Act requires notification to customers in the event of a security breach of customer's computerized data, specifically customer's personally identifiable information (PII). The	BCC Ch. 521

	notification must be done as quickly as possible. The Act does provide for remedies not to exceed $50,000 per violation. If more than 10,000 individuals were affected by a breach, consumer reporting agencies must be notified. The Act does have a safe harbor when data is protected with encryption.	
Texas Medical Records Privacy Act	The Texas Medical Records Privacy Act is Texas law making Protected Health Information confidential. This law is applicable to "Texas covered entities" or "any person who… comes into possession of protected health information," a term more broadly defined than HIPAA's "Covered Entities" and "Business Associates" (collectively: healthcare providers, healthcare clearing houses, health plans, and any business associates of the aforementioned).	HSC Ch. 181
Texas Administrative Code	Information Security Standards for State Agencies and Institutions of Higher Education.	1 TAC 202
	Administrative rule pertaining to agencies' websites.	1 TAC 206
	Each agency and institution of higher education must protect the privacy and personal identifying information (PII) of a member of public who provide or receive information from or through the institution's website. Prior to providing access to information or services on a state website that requires PII, each institute must conduct a transaction risk assessment and implement appropriate safeguards that conform to TAC 202.	1 TAC § 206.52, 1 TAC § 206.72
	Texas rule in line with HIPAA, Privacy of Health Information, etc.: provides for the privacy of health information, an individual's right to correct such information, and the process for doing so.	25 TAC § 1(W)

10.2 Federal Laws and Regulations for Data Privacy and Security

Health Insurance Portability and Accountability Act (HIPAA) (1996)	HIPAA contains the following provisions regulating the use and disclosure of protected health information: • *Privacy Rule* protects the privacy of individually identifiable health information; • *Security Rule* sets national standards for the security of electronic protected health information;	HIPAA (1996);

	• *Breach Notification Rule* requires covered entities and business associates to provide notification following a breach of unsecured protected health information; • *Enforcement* providing civil and criminal penalties for violation; and • *Patient Safety Rule* protects identifiable information being used to analyze patient safety events and improve patient safety.	
Health Information Technology for Economic and Clinical Health Act (HITECH) (2009)	HITECH amended HIPAA in 2009 with interim regulations, expanding direct liability to HIPAA Business Associates and requiring Covered Entities and Business Associates to report data breaches to those affected individuals through specific breach notification requirements.	HITECH (2009) (ARRA Title XIII)
HIPAA Omnibus Regulations (2013)	These regulations made substantial changes to HIPAA: • The Omnibus Regulations finalized the interim HITECH regulations; • Made Business Associates directly liable for certain Privacy and Security requirements; • Enacted stronger prohibitions on marketing (opt-out) and sale of Protected Health Information (PHI) without authorization; • Expanded individuals' rights to receive electronic copies of PHI; • Allowed individuals the right to restrict disclosures to a health plan concerning treatment for which the individual has paid out-of-pocket in full; • Required Notice of Privacy Practices updates and redistribution; • Changed authorization related to research and disclosure of school proof of child immunization and access to decedent information by family members or others; • Enhanced enforcement in many ways, including addressing the enforcement against noncompliance with HIPAA Rules due to willful neglect; • Finalized the rule adopting changes to the HIPAA Enforcement Rule to incorporate tiered, mandatory penalties up to $1.5 million per violation; and • Finalized rule adopting GINA and prohibited most health plans from using or disclosing genetic information for underwriting purposes, as proposed in Oct. 2009.	45 CFR Parts 160-164
Family Educational Rights and	FERPA creates a right of privacy regarding grades, enrollment, and billing information. Specifically, this information may not be released without prior consent	20 USC § 1232G; 34 CFR Part 99

Privacy Act (FERPA) (1974)	from the student. In addition to safeguarding individual student records, the law also governs how state agencies transmit testing data to federal agencies.	
Federal Information Security Management Act (FISMA) (2006)	Federal legislation that assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to provide for the strengthening of information security systems. Specifically, the Act requires heads of each agency to implement policies and procedures to effectively and efficiently drive down IT security issues to acceptable levels through a defined framework by which federal government agencies would ensure the security of information systems controlled by either the agency or one of its contractors on behalf of a federal agency. The framework is further defined by the standards and guidelines set forth by NIST.	44 USC §§ 3541-3549
Internal Revenue Service Statute and Regulation	Through Publication 1075, the IRS has created a framework by which Federal Tax Information (FTI) and Personally Identifiable Information (PII) is protected from public disclosure. To ensure the safety of such data, receiving agencies and/or entities must have proper safeguards in place. Federal code requires external agencies and other authorize recipients of federal tax return and return information (FTI) to establish specific procedures to ensure the adequate protection of the FTI they receive. In addition, the same section of the Code authorizes the IRS to suspend or terminate FTI disclosure to a receiving agency or other authorized recipient if misuse or insufficient FTI safeguards are found. In addition to criminal sanctions, the Internal Revenue Code prescribes civil damages for unauthorized disclosure and, when appropriate, the notification to affected taxpayers that an unauthorized inspection or disclosure has occurred.	Publication 1075; IRC Section 6103(p)(4); 26 USC §6103(p)(4)
Social Security Administration (SSA) Statute and Regulation	Much of the information SSA collects and maintains on individuals is especially sensitive, therefore prior to disclosing of such information, SSA must look to the Privacy Act of 1974, 5 USC Section 552a, FOIA, 5 USC Section 1106 of SSA, 42 USC Section 1306. SSA employees are prohibited from disclosing any information contained in SSA records unless disclosure is authorized by regulation or otherwise required by federal law. SSA may only disclose personal records (PII) when the individual to whom the record pertains provides written consent or when such disclosure falls into one of the several narrowly-drawn exceptions.	Privacy Act of 1974; 5 USC Section 552a; FOIA; 5 USC §1106 (SSA); 42 USC §1306

National Institute of Standards and Technology (NIST)	NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and to help with managing cost effective programs to protect their information systems and the data stored on the systems. NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in FIPS 200. The security rule covers 17 areas, including control, incident response, business continuity, and disaster recoverability. A key part of the certification and accreditation process for federal information systems is selecting and implementing a subset of the controls. Agencies are expected to comply with NIST security standards and guidelines.	NIST 800-53 rev. 4; FIPS 200
Criminal Justice Information Services (CJIS)	CJIS is a division of the FBI that compiles data provided by law enforcement agencies across the United States. CJIS is the world's largest repository of criminal fingerprints and history records which can be accessed and searched by law enforcement to enable the quick apprehension of criminals. The responsibility of CJIS extends to the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Incident-Based Reporting System (NIBRS). In addition to its many responsibilities in the coordination and sharing of criminal data, CJIS promulgates the CJIS Security Policy, which is meant to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI). The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. The policy applies to every individual – contractor, private entity, noncriminal justice agency representatives, or members of a criminal justice entity – with access to, or who operate in support of, criminal justice services and information.	CJIS Security Policy, TGC § 552.108
Clinical Laboratory Improvements Amendments (CLIA)	CLIA are federal regulatory standards applying to clinical laboratory testing performed on humans in the United States. The CLIA Program sets standards and issues certificates for clinical laboratories. The objective of CLIA is to ensure the accuracy, reliability, and timeliness of test results regardless of where the test is performed. All clinical laboratories must be properly certified to receive Medicare and Medicaid payments. The primary responsibility for the administration of this program is held by the Centers for Medicare and Medicaid Services.	CLIA Regulations and Guidance

Computer Fraud and Abuse Act (CFAA)	CFAA is a federal law passed to address computer-related crimes. The Act governs cases with a compelling federal interest; where computers of the federal government or certain financial institutions are involved; where the crime is interstate in nature; or where computers are used in interstate and foreign commerce. The CFAA defines "protected computers" as those exclusively used by financial institutions or the US Government, or when the conduct constituting the offense affects the use by or for the financial institution or the federal government, or those computers which are used in or affecting interstate or foreign commerce or communication.	18 USC §1030

10.3 Other Laws and Regulations for Data Privacy and Security

General Data Protection Regulation (GDPR) (2018)	The General Data Protection Regulation (GDPR) is a privacy and security law drafted and passed by the European Union (EU). It imposes obligations onto organizations across the globe, so long as they target or collect data related to people in the EU. The GDRP includes many key regulatory points, including: • Data protection principles • Accountability • Data security • Data protection by design and by default • When you're allowed to process data • Consent • Data Protection Officers • Privacy rights	**GDPR (2018)**

Acknowledgements

Version 1 of the Incident Response Form was published on behalf of the Department of Information Resources, with the input of the Statewide Information Security Advisory Committee, Privacy Advisory Committee, Data Breach Response Subcommittee. The members included:

Co-Chair: Sheila Stine, JD, Health and Human Services Commission, Chief Privacy Officer

Co-Chair: Martin Zelinsky, JD, Department of Information Resources, General Counsel

Chad Lersch, JD, Department of Information Resources, Assistant General Counsel

Betsy Loar, JD, Credit Union Department, Assistant Commissioner and General Counsel

Shelley Janda, JD, Department of Aging and Disability Services, Assistant General Counsel

Susan Maldonado, JD, Texas Facilities Commission, Assistant General Counsel

Their participation in creating this document is appreciated.

The current version of this document is maintained by the Department of Information Resources, Chief Information Security Office.