

TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
TDHCA Governing Board Approved Draft of Proposed New
10 TAC §1.24, Information Security and Privacy Requirements

Disclaimer

Attached is a draft of proposed new 10 TAC §1.24, Information Security and Privacy Requirements, that was approved by the TDHCA Governing Board on April 25, 2019. This document, including its preamble, is expected to be published in the May 10, 2019, edition of the Texas Register and that published version will constitute the official version for purposes of public comment and can be found at the following link: <https://www.sos.texas.gov/texreg/index.shtml>.

Public Comment

Public Comment Period: Start: 8:00 a.m. Austin local time on May 10, 2019
End: 5:00 p.m. Austin local time on June 10, 2019

Comments received after 5:00 p.m. Austin local time on June 10, 2019, will not be accepted.

Written comments may be submitted, in hard copy/fax or electronic formats to:

Texas Department of Housing and Community Affairs
Attn: Brooke Boston
Rules Comments
P.O. Box 13941
Austin, Texas 78711-3941
Email: brooke.boston@tdhca.state.tx.us

Written comments may be submitted in hard copy or email formats within the designated public comment period. Those making public comment are encouraged to reference the specific draft rule, policy, or plan related to their comment as well as a specific reference or cite associated with each comment.

Please be aware that all comments submitted to the TDHCA will be considered public information.

TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
Street Address: 221 East 11th Street, Austin, TX 78701
Mailing Address: PO Box 13941, Austin, TX 78711-3941
Main Number: 512-475-3800 Toll Free: 1-800-525-0657
Email: info@tdhca.state.tx.us Web: www.tdhca.state.tx.us

Preamble, including required analysis, for proposed new 10 TAC §1.24, Information Security and Privacy Requirements

The Texas Department of Housing and Community Affairs (the Department) proposes new 10 TAC §1.24, Information Security and Privacy Requirements. The purpose of the proposed rule is to expand the rule beyond only protected health information to other non-health protected information, and to provide a more detailed definition of the duties and responsibilities of contractors who handle that protected information on behalf of the Department. The proposed rule will be newly titled Information Security and Privacy Requirements, and addresses all types of protected information that the Department encounters, and sets forth specific requirements of contractors for the protection of such information.

Tex. Gov't Code §2001.0045(b) does not apply to the rule being proposed under exception item (6) which provides for an exception when necessary to protect the health, safety, and welfare of the residents of this state. Through protection of private information, the welfare of residents is protected. No costs are associated with this proposed rule.

The Department has analyzed this rulemaking and the analysis is described below for each category of analysis performed.

a. GOVERNMENT GROWTH IMPACT STATEMENT REQUIRED BY TEX. GOV'T CODE §2001.0221.

David Cervantes, Acting Director, has determined that, for the first five years the proposed rule will be in effect:

1. The new rule does not create or eliminate a government program, but relates to the re-adoption of this rule which makes changes to the rule governing the security of personal information.
2. The new rule does not require a change in work that would require the creation of new employee positions, nor will it reduce work load to a degree that eliminates any existing employee positions.
3. The new rule changes do not require additional future legislative appropriations.
4. The new rule will not result in an increase in fees paid to the Department, nor in a decrease in fees paid to the Department.
5. The new rule is not creating a new regulation, except that it is replacing a rule being repealed simultaneously to provide for revisions.
6. The rule will not limit, expand, or repeal an existing regulation but merely revises a rule.
7. The new rule does technically increase the number of individuals to whom this rule applies, as several new provisions are being specified; however, those Contractors subject to those provisions of the rule are already required to satisfy the state and federal regulations specified. This rule merely formalizes these requirements in one place, under rule, and provides the specific detail on the agreement required of Contractors reflecting their adherence to the requirements.
8. The new rule will not negatively nor positively affect the state's economy.

b. ADVERSE ECONOMIC IMPACT ON SMALL OR MICRO-BUSINESSES OR RURAL COMMUNITIES AND REGULATORY FLEXIBILITY REQUIRED BY TEX. GOV'T CODE §2006.002.

1. The Department has evaluated this rule and determined that none of the adverse affect strategies outlined in Tex. Gov't Code §2006.002(b) are applicable.

2. This rule provides specific detail on the handling by Department Contractors of personal information. Contractors subject to those provisions of the rule are already required to satisfy the state and federal regulations specified. This rule merely formalizes these requirements in one place, under rule; and provides the specific detail on the agreement required of Contractors reflecting their adherence to the requirements. Other than in the case of a small or micro-business that participates as a Contractor in one of these programs, no small or micro-businesses are subject to the rule. If a small or micro-business does participate as a Contractor in a program, the requirements of the rule – already provided for in other state and federal regulations – will not require an onerous burden.

3. The Department has determined that because this rule relates only to a revision to a rule, and the rule changes do not specifically relate to geographic location or business size, there will be no economic effect on small or micro-businesses or rural communities.

c. TAKINGS IMPACT ASSESSMENT REQUIRED BY TEX. GOV'T CODE §2007.043. The new rule does not contemplate nor authorize a taking by the Department, therefore no Takings Impact Assessment is required.

d. LOCAL EMPLOYMENT IMPACT STATEMENTS REQUIRED BY TEX. GOV'T CODE §2001.024(a)(6).

The Department has evaluated the rule as to its possible effects on local economies and has determined that for the first five years the rule will be in effect the new rule has no economic effect on local employment because this rule relates only to requirements of existing and future Department Contractors and echoes state and federal regulations already in effect.

Texas Gov't Code §2001.022(a) states that this "impact statement must describe in detail the probable effect of the rule on employment in each geographic region affected by this rule..." Considering that the rule is applicable to all properties statewide, there are no "probable" effects of the new rule on particular geographic regions.

e. PUBLIC BENEFIT/COST NOTE REQUIRED BY TEX. GOV'T CODE §2001.024(a)(5). Mr. Cervantes has determined that, for each year of the first five years the new sections are in effect, the public benefit anticipated as a result of the proposed new rule will be a clearer rule for Contractors and improved assurance of the safety and security of personal information. There will be limited economic cost to any individuals required to comply with the proposed new rule because the activities described by the rule are already applicable under other state and federal regulations.

f. FISCAL NOTE REQUIRED BY TEX. GOV'T CODE §2001.024(a)(4). Mr. Cervantes also has determined that for each year of the first five years the new sections are in effect, enforcing or administering the new sections does not have any foreseeable implications related to costs or revenues of the state or local governments as the implementation of this rule generates no fees, nor requires any cost.

REQUEST FOR PUBLIC COMMENT. The public comment period will be held May 10, 2019, to June 10, 2019, to receive input on the proposed new rule. Written comments may be submitted to the Texas Department of Housing and Community Affairs, Attn: Brooke Boston, Rule Comments, P.O. Box 13941, Austin, Texas 78711-3941 or

brooke.boston@tdhca.state.tx.us. ALL COMMENTS MUST BE RECEIVED BY 5:00 p.m., Austin local time, June 10, 2019.

§1.24, Information Security and Privacy Requirements~~Protected Health Information~~

(a) Purpose.

The purpose of this rule is to provide the mechanism by which the Department will ensure the security and privacy of Protected Information belonging to persons who do business with the Department and those they serve.

(b) Definitions.

The following words and terms, when used in this subchapter, shall have the following meanings, unless the context clearly indicates otherwise.

(1) Affiliate--Shall have the meaning assigned by the specific program or programs described in this title.

(2) Computing Device--Any computer, laptop, server, smart phone, or any other data processing device that is used to connect to the Department's network.

(3) Contractor--A third party, including, but not limited to, outside auditors and legal counsel, funding agencies, Vendors or Subrecipients, including any and of its Representatives that may gain access to Protected Information on account of a contract with the Department.

(4) Criminal History Records Information--For the purposes of Tex. Gov't Code Chapter 411, Subchapter F, information collected about a person by a Criminal Justice Agency that consists of identifiable descriptions and notations of arrests, detentions, indictments, information, and other formal criminal charges and their dispositions. The term does not include:

(A) identification information, including fingerprint records, to the extent that the identification information does not indicate involvement of the person in the criminal justice system; or

(B) driving record information under Subchapter C, Chapter 521 Transportation Code.

(5) Department--The Texas Department of Housing and Community Affairs.

(6) Financial Statements of a Tax Credit Applicant--For purposes of Tex. Gov't Code §2306.6717(d)(Public Information and Hearings), a formal statement of the financial activities of a Low Income Housing Tax Credit Applicant, submitted to the Department as part of a Low Income Housing Tax Credit Application, including but not limited to, the balance sheet, income statement, cash flow statement or changes in equity.

(7) Information Resources--The procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

(8) Information Security and Privacy Agreement (ISPA)--An agreement between the Department and a Contractor implementing information security and privacy requirements of the Department.

(9) Non-Public Personal Information--For purposes of the Graham-Leach-Bliley Act (15 USC §§6801-6809 and 6821-6827), and implementing regulations, personally identifiable financial information provided to the Department or any of its Contractors, resulting from any transaction with, or any service performed for a client or consumer, or otherwise obtained by the Department or its Contractors, unless the information is otherwise publically available.

(10) Personal Identifying Information--For purposes of TEX. BUS. & COM. CODE Chapter 521 (Unauthorized Use of Identifying Information), and any implementing regulations, 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 fingerprint, voice print, retina or iris image, unique electronic identification number, address, or routing code, and telecommunication access devices as defined by Tex. Penal Code §32.51.

(11) Personal or Business Financial Information--For purposes of Tex. Gov't Code §2306.039 (Open Meetings and Open Records), any personal or business financial information including, but not limited to, Social Security numbers, tax payer identification numbers, or bank account numbers submitted to the Department to receive a loan, grant, or other housing assistance by a housing sponsor, individual or family.

(12) Protected Health Information--For purposes of Tex. Health & Safety Code Chap. 181 (adopting definitions in 45 CFR §160.103), any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and that identifies the individual, or can be used to identify the individual.

(13) Protected Information--Protected Health Information, Personal Identifying Information, Sensitive Personal Information, Personal or Business Financial Information, Non-Public Personal Information, Financial Statement of a Tax Credit Applicant, WAP Applications and Participation Information, Criminal History Records Information, and Victims of Violence Information.

(14) Representative--Any officer, employee, contractor, subcontractor, member, director, advisor, partner, or agent of Vendor/Subrecipient, or any person serving in such a role, however titled or designated.

(15) Sensitive Personal Information--For purposes of TEX. BUS. & COM. CODE Chapter 521 (Unauthorized Use of Identifying Information), 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 or government-issued identification number,

(C) account or credit/debit card number in combination with any required security code, access code, or password that would permit access, or

(D) information that identifies or reveals an individual and the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual.

(E) The term does not include publicly available information that is lawfully made publicly available.

(16) Subrecipient--Includes any entity receiving funds or awards from the Department. An organization with whom the Department contracts, and entrusts to administer federal or state programs or funds, including but not limited to, units of local government, non-profit and for-profit corporations, administrators, community action agencies, collaborative applications, subgrantees, developers, owners, land banks, participating mortgage lenders, and non-profit owner-builder housing providers. This also includes an Affiliate of a Subrecipient.

(17) Vendor--A person or organization that supplies goods or services, properly procured under relevant laws, to the Department.

(18) Victims of Violence Information--Any information submitted to a covered housing provider, including the Department and its Contractors pursuant to 24 CFR §5.2007, including the fact that an individual is a victim of domestic violence, dating violence, sexual assault, or stalking. Also included pursuant to Tex. Gov't Code §552.138 is information regarding the location or physical

layout, an employee, volunteer, former or current client, or the provision of services to a former or current client, a private donor, or a member of a board of directors or board of trustees of a family violence shelter center, victims of trafficking shelter center, or sexual assault program.

(19) WAP Applications and Participation Information--For purposes of Weatherization Program Notice 10-08, U.S. Department of Energy, issued February 1, 2010, regarding the Department of Energy Weatherization Assistance Program (WAP), any specifically identifying information related to an individual's eligibility application for WAP or the individual's participation in WAP, such as name, address, or income information.

(c) Applicability and Implementation.

(1) This rule applies to Contractors as defined in §1.24 (b). This rule is not applicable to third parties that contract with the Department but have no access to Department Protected Information.

(2) Contractors with Department contracts that are active on the effective date of this rule shall have 180 calendar days from the effective date of this rule to enter into an ISPA with the Department. Contractors that execute new Department contracts or contract renewals on or after the effective date of this rule shall enter into an ISPA with the Department no later than the date of contract execution, if an ISPA with the Department is not already in place. The ISPA shall be in a form provided by the Department on its website. A Contractor must download, execute and return the contract according to instructions on the website. A Contractor need only execute one ISPA, even if they participate with the Department in multiple programs or activities.

(3) The ISPA shall be effective with respect to all current and future contracts that Contractor has or will have with the Department for as long as the Contractor has access to Protected Information. Contractors receiving awards or contracts after the effective date of this rule must have an executed ISP Agreement on file with the Department or enter into an ISP Agreement before work can begin on the new award or contract.

(4) Contractor and Department may agree to eliminate or reduce access to, or the generation of, any class of Protected Information related to Contractor's obligations to the Department, provided it does not impair Contractor's ability to fulfill its obligations to the Department.

(5) Contractor shall accept responsibility for all Representatives and ensure the safeguarding of Protected Information in accordance with applicable federal and state laws, and the terms and conditions set forth in the ISPA.

(6) The Department may, in its sole discretion, require Contractor to amend an ISPA in order to conform to state and/or federal law.

(d) ISPA Security Measures

The ISPA shall include, among other requirements:

(1) security measures for devices that connect to the Department network, and

(2) security measures for maintenance of Department information external to the Department network, including, but not limited to:

(A) maintaining an inventory of all information technology (IT) assets;

(B) implementing and maintaining a risk management program;

(C) ensuring information is recoverable in accordance with risk management decisions;

(D) adhering to monitoring techniques for detecting, reporting, and investigating security incidents;

(E) providing IT security training to employees;

(F) conducting criminal background checks on employees with access to department information;

(G) separating development and production environments;

(H) following a software change control process;

(I) maintaining and following an IT security policy that has been approved by the department;
and

(J) implementing other requirements reasonably necessary to ensure the security and privacy of Protected Information in the Contractor's possession or control.

(e) Breach.

In the event of an actual or suspected breach involving Department Private Information stored by the Contractor, Contractor shall promptly notify the Department no later than twenty-four hours after discovery of the incident. The Contractor will coordinate and cooperate fully with the Department in making all breach notifications and taking all actions required by law to effect the required notifications.

(f) Texas Public Information Act.

If Contractor receives a request pursuant to the Texas Public Information Act for Information maintained by Contractor on account of a contract with TDHCA, Contractor shall notify the Department within three calendar days of the receipt of the request by forwarding the request to open.records@tdhca.state.tx.us

(g) Department Review.

Contractor and Representatives shall permit Department to conduct periodic IT general controls audits, Internet security scans, and internal network vulnerability assessments, and contract monitoring audits at reasonable times, and upon reasonable notice. Such reviews may be conducted by the Department, the Texas State Auditor's Office, the Texas Department of Information Resources, an applicable federal oversight agency, or any third parties under contract with one of these agencies.