Health and Human Services
Acceptable Use Agreement (AUA)
(Formerly known as the Computer Use Agreement or CUA)

Please read the following agreement carefully and completely before signing.

Purpose

The purpose of this document is toinform you of your responsibilities concerning the use of Texas Health and Human Services System (HHS) Confidential Information, HHS Agency sensitive information, and HHS Information Resources.[1] This includes: computer, hardware, software, infrastructure, data, personnel, and other related resources. Your signature is required to formally acknowledge your understanding, acceptance, and compliance of HHS's Information Resource Acceptable Use provisions. This agreement applies to all persons using HHS Information Resources and/or using, disclosing, creating, transmitting, or maintaining HHS Confidential Information or HHS Agency sensitive information, whether employed by an HHS Agency or not, and is based on policy delineated in the HHS Enterprise Information Security Policy (EIS-Policy), and the HHS Enterprise Information Security Acceptable Use Policy (EIS-AUP). Users are further informed of their responsibilities regarding the use of HHS Information Resources when taking the required annual *HHS Enterprise Information Security Acceptable Use Training.*

I understand and hereby agree to comply with the following Information Resource Acceptable Use provisions:

Authorized Use

- Information Resources are intended to be used in support of official state-approved business.
- Limited personal use of Information Resources may be allowed and is described in other policies and procedures of the HHS Agency by which I am employed.
- Proper authorization is required for access to all information owned by HHS Agencies, except for information that is maintained for public access.
- I will not attempt to access or alter any information that I am not authorized to work with in the performance of my job duties.
- I will not enter any unauthorized information, make any unauthorized changes to information, or disclose any information without proper authorization. Unauthorized access to an HHS Information Resource, allowing another party unauthorized access to, or maliciously causing a computer malfunction are violations under Chapter 33 of the Texas Penal Code ("Computer Crime Law") and are punishable by fines, jail time, or both.

User Credentials

- I will receive and will be required to use credentials (User ID and Password) to gain access to and to use HHS Information Resources.
- I will employ a difficult to guess password with a minimum of eight characters in length containing upper case alpha, lower case alpha, numerical, and special characters unless further requirements for passwords are issued.
- I will not construct my password from obvious user names or passwords, such as personal information (i.e. telephone numbers, relative's names, pet's names, or passwords used for personal business, etc.).
- Under no circumstances will I allow my credentials to be used by any other individual, nor will I use

[1] As defined in HHS EIS-Definitions document:
§2054.003(7), Texas Government Code.
Information resources" means 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.
And as defined in [44 U.S.C., Sec. 3502], NIST SP 800-53 rev 4.
Information and related resources, such as personnel, equipment, funds, and information technology.

credentials belonging to someone else.

- I will be held responsible for any violations of applicable law or agency policy related to HHS Confidential Information, HHS Agency sensitive information, or HHS Information Resources, caused by my acts or omissions, or for any harm, loss, or adverse consequences arising from the use of my credentials, including any unauthorized use by a third party or contractor if such party gains access to my credentials due to my negligence or misconduct. Disciplinary actions up to and including dismissal and civil or criminal prosecution may result from any violations or misuse.
- Transactions initiated under my credentials will be considered as having been authorized and electronically signed by me.
- I will not disclose my password to anyone.

Software

- Only properly licensed software may be used on HHS Information Resources.
- I will use all software installed on HHS Information Resources in a manner that complies with the terms of the applicable software license agreement and all applicable law and HHS Agency policies and procedures.
- I will not install or use any software on HHS Information Resources that has not been approved for use in accordance with HHS Agency policies and procedures.

HHS Confidential Information

HHS Confidential Information includes information from the IRS (Federal Tax Information (FTI)) or the Social Security Administration (SSA), personally identifiable information, such as patient/client identifying health information, employee information, unpublished agency work product, or any information (patient or otherwise) that is classified confidential by applicable law and HHS Agency policy. You may have authority to use or disclose some or all of this HHS Confidential Information only as an authorized person through a computer system, or in paper or oral form or for your work for authorized purposes.

HHS Confidential Information is valuable and sensitive, and is protected by law and by HHS policies. The intent of these laws and policies is to safeguard the information against unauthorized use or disclosure and in support of the organization's mission. As a user of HHS systems and HHS Confidential Information, you are required to conform to applicable laws and HHS policies governing confidential information. Your principal obligations in this area are outlined below. You are required to read and to abide by these obligations.

I understand that in the course of my job, I may have authority to use or disclose HHS Confidential Information related to:

- Individuals' personally identifiable information about patients/clients (such as records, conversations, admissions information, diagnosis, prognosis, treatment plan, financial information, or other identifiers such as name, social security number, benefit plan, etc.) HHS Workforce personally identifiable information including home addresses, home phone numbers, and social security numbers. HHS Workforce includes employees, interns, trainees, volunteers, and staff augmentation contractors.
- HHS Agency functions (such as unpublished or draft financial information, internal reports, memos, contracts, peer review information, communications, proprietary computer software, and procurement information).
- Legal work product or other information deemed confidential under applicable law or HHS Agency policy.
- Contractor or third party information (such as vendor information).

Accordingly, as a condition of my access to HHS Confidential Information, I agree that:

- I will use HHS Confidential Information only as needed to perform legitimate duties. This means, among other things, that:

- I will only access HHS Confidential Information that I have a need to know;
- I will not in any way create, use, disclose, transmit, maintain, copy, sell, loan, review, alter, or destroy any HHS Confidential Information except as properly authorized within the scope of my duties for HHS;
- I will not misuse or carelessly handle HHS Confidential Information; and
- I will encrypt HHS Confidential Information when appropriate, including when emailing such information and when storing such information on portable storage devices. I will not use confidential individual identifiers in email subject lines because subject lines are never encrypted.
- I will safeguard and will not disclose my user name or password or any other authorization I have that allows me to access to HHS Confidential Information, except as permitted by law and applicable HHS Agency policy.
- I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity or availability of HHS Confidential Information to my supervisor and the HHS Privacy Office at: privacy@hhsc.state.tx.us or (877) 378-9869 or the agency's Privacy Office. I will immediately report computer security incidents to the help desk.
- Reports are made in good faith about suspect activities and will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities. Retaliation for a good faith report of a violation of law or policy is prohibited by HHS.
- My obligations under this Agreement will continue after termination of my association with HHS or access to HHS applications until all HHS Confidential Information in my possession, custody or control is returned or destroyed as directed by HHS.
- My privileges hereunder are subject to periodic review, revision, and if appropriate, removal.
- I have no right or ownership interest in any HHS Confidential Information referred to in this Agreement. HHS may revoke my access code or other authorized access to HHS Confidential Information at any time.
- I will, at all times, safeguard and retain the confidentiality, integrity and availability of HHS Confidential Information.
- I acknowledge my responsibility to be aware of, read, and comply with HHS security policy, standards, and controls[2].

Agency Sensitive Information

Agency sensitive information is information that is not subject to specific legal, regulatory or other external requirements, but is considered HHS sensitive and should not be readily available to the public. Agency sensitive information must be protected even though disclosure is not specifically restricted by legal or regulatory requirements.

Examples of agency sensitive information include but are not limited to:

- HHS-specific legal information such as nondisclosure agreements (NDAs) and contracts.
- Unpublished financial information related to organizational accounting such as balance sheets, purchase orders, contracts and budget information.
- Unpublished financial information related to employee compensation, such as offer letters, salaries, severance, retirement plans, and benefits.
- Internal operational procedures.

Some information, even though it is available to the public, may contain sensitive information. Consequently, I understand it is also my responsibility to protect this information according to its sensitivity, value, and impact to HHS.

I understand that my failure to comply with this Agreement may result in loss of access privileges to HHS applications; disciplinary action, up to and including dismissal; and civil or criminal prosecution.

If I receive a request for the public disclosure of information, I will follow my agency's policies and procedures for the release of public information.

[2] HHS security policy, standards, and controls can be found at http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

Health and Human Services
Acceptable Use Agreement (AUA)
(Formally known as the Computer Use Agreement or CUA)

Workforce Nondisclosure and Procurement Integrity Statement

As an HHS workforce member (employee, trainee, intern, volunteer or staff augmentation contractor) of the Texas Health and Human Services Commission (HHSC) or a Health and Human Services (HHS) agency, I may be provided access to HHS Confidential Information or agency sensitive information regarding the proposed work, procurement of goods and services for HHSC or an HHS Agency. As such, I acknowledge that:

- My access to this information is authorized only within my duties as an HHS Workforce Member of HHSC or an HHS Agency;
- My access to this information is solely for the purpose of discharging the duties of HHSC or an HHS Agency regarding the proposed procurement;
- Premature or unauthorized disclosure of this information will irreparably harm the State's interests in the proposed procurement and may constitute a violation of *Section 39.02 of the Texas Penal Code*, the antitrust laws of the United States and the State of Texas, and the *Texas Public Information Act, Chapter 552, Texas Government Code*; and
- The information may represent confidential or proprietary information, the release of which may be restricted or prohibited by law.

In view of the foregoing, I agree that I shall only use, disclose, create, maintain or transmit any information that I receive in my capacity as an HHS workforce member, in any form, whether electronic, paper or oral, formal or informal – for the following authorized purposes only:

- To provide the goods, services and/or deliverables required or requested under this HHSC or HHS Agency procurement in accordance with my assigned duties;
- To provide action, response or recommendation requested by HHSC or an HHS Agency in the course of fulfilling my assigned duties regarding the proposed procurement as prescribed under the resulting contract;
- To evaluate the submissions received from vendors or offerors in connection with the proposed procurements in accordance with my assigned duties;
- To assist HHSC or an HHS Agency in developing any documents, reports, working papers, evaluations, schedules, or instruments necessary to fulfill the requirements of the procurement; or
- As otherwise authorized in writing by HHS.

I further agree that I will regard any such information as confidential and that I will not use, disclose, create, transmit or maintain the information or any summary or synopsis of the information in any manner or any form whatsoever, except under the following circumstances:

- When authorized in writing by an HHSC or HHS employee associated with the respective proposed procurement or my assigned duties at HHS;
- When required by law as determined by HHS Legal Counsel;
- When the information has previously been released to the general public by HHSC or an HHS Agency regarding the respective proposed procurement -provided such release was not inadvertent or unintentional; and
- When required, to brief or inform a manager or supervisor, provided the manager or supervisor is informed of and agrees to the limitations on further disclosure contained in this statement.

In the event I receive a request for information relating to a proposed procurement either during or after the performance of this resulting contract, I agree to do the following:

- Notify HHSC or HHS Agency Information Owner associated with the respective proposed procurement as soon as practical following receipt of the request, who will seek advice from appropriate legal counsel and further instruct me regarding my ability to disclose the information.

The aforementioned statements supersede any other non-disclosure statement related to a proposed procurement or work duties. Any prior authorizations relating to access to information related to a proposed procurement are revoked.

In addition, I agree to notify the HHSC or HHS Agency employee associated with the respective proposed procurement immediately if I learn or have reason to believe that any information covered by this Workforce Nondisclosure and Procurement Integrity Section has been disclosed, intentionally or unintentionally, by any person.

Physical Security

- I will not use, disclose, transmit, maintain, create or remove Information Resources or HHS Confidential Information or HHS Agency sensitive information from HHS property without proper prior authorization and approval of supervisory HHS staff.
- I will immediately report the loss or theft of any Information Resource or information to the appropriate investigative office in accordance with all HHS Agency policies and procedures.
- I will secure my workstation either by logging off or locking my screen when away from my workstation.
- I will keep HHS Information Resources under my physical control at all times, or will safeguard them when away, such as by keeping my workspace clean, not leaving HHS Confidential Information, HHS Agency sensitive information, or Information Resources in my vehicle unattended and locking Information Resources with a locking cable or a suitable locked container under my control.

E-Mail

- I understand that the state government e-mail system is provided for official HHS business.
- I will limit my incidental, non-official use of the e-mail system to prevent interference with my official duties or cause degradation of network services, in accordance with HHS Agency policy.
- I will not send e-mail that violates HHS Agency policy, such as e-mail that contains malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or inappropriate racial, gender, sexual, or religious content over state government e-mail.
- I will not use personal email accounts (e.g. Gmail, Hotmail, Yahoo etc.) for transmitting or receiving HHS Agency information or conducting agency business.
- I will utilize HHS Agency approved encryption for transmitting HHS Confidential Information.

Internet

- I understand that access to public networks (i.e. the Internet) is for official HHS business.
- I will limit my incidental, non-official access to the Internet to prevent interference with my official duties or cause degradation of network services, in accordance with HHS Agency policy.
- I will not view or attempt to view web content that violates HHS policy, such as sites known to contain malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or inappropriate racial, gender or sexual content, text or graphics.
- I will not utilize unapproved cloud computing resources or storage unless approved by HHS. These include but are not limited to Apple iCloud, Dropbox, Google Docs, or any other commercially available cloud computing service that is not expressly approved by HHSC IT.
- I will not use a personal or public available proxy to circumvent security policies for internet usage.

Social Media

I understand from the HHS Social Media Policy, that incidental, non-work related use of social networking sites such as Facebook, Myspace, Twitter, and video-hosting sites such as YouTube are prohibited. Exceptions for the use of social media sites for approved HHS business purposes must be approved by their agency's Office of Communications or an employee designated by the agency's Commissioner to authorize social media use before establishing each new social media presence on the agency's behalf.

Instant Messaging

I understand that the only approved Instant Messaging (IM) system is HHS provided Instant Messaging from

Microsoft. Use of other Instant Messaging systems is prohibited except for specific instances approved by an Information Resources Manager (IRM) for HHS Agency business purposes. Policies relating to Instant Messaging can be found in the *HHS Policy for Use of Agency-Provided Instant Messaging*[3].

Non-Agency Devices

The following is only applicable if your agency has a Bring Your Own Device (BYOD) program:

I understand the Bring Your Own Device (BYOD) program, if offered by my agency, is an opt-in (voluntary) decision and requires that my agency have certain control over my personal or non-HHS owned device (smartphone, tablet, or laptop) in exchange for access to HHS Confidential Information or Information Resources such as the network and email. I may opt-out of the BYOD program at any time.

I must meet Bring Your Own Device (BYOD) eligibility, device requirements, and obtain management approval in order to participate in the BYOD program.

I understand HHS has no responsibility for my BYOD devices and associated costs, to include, but not limited to, vendor terms and conditions; sufficient data and call plan, service levels, calling areas, service and phone features, termination clauses, and payment terms and penalties. I am also responsible for the purchase, loss, damage, insurance, and/or replacement.

I will notify the help desk immediately if my BYOD device is lost or stolen, if there is a privacy or security incident associated with my device containing HHS information, or if there are plans to replace or sell my BYOD equipment.

I understand that HHS, at its sole discretion, can utilize information on a BYOD device as it determines is required or would be helpful to the organization to gather data on usage of mobile devices; ensure compliance with organization policies; gather information for internal investigations or review; and to respond to informational requests in litigation or government investigations.

I understand that if I am a Fair Labor Standards Act (FLSA) nonexempt employee, performing work under the BYOD or other program or technology that makes accessing work convenient from any location or time, that I am required to log all hours worked as required and prescribed by the applicable HHS's Human Resources (HR) policy.

I understand that if I am a Supervisor of FLSA Non Exempt employee's, I will assure that FLSA Non Exempt employee's performing work under the BYOD or other program or technology that makes accessing work convenient from any location or time will not be required to work after their assigned hours unless directed by their supervisor or manager.

Additional information on employee responsibilities associated with the BYOD program can be found on the IT policy website[4].

Consent to Monitoring

I understand that HHS has the legal right to monitor use of HHS Information Resources, HHS Confidential Information, and HHS Agency sensitive information and that HHS monitors use to ensure these resources are protected and to verify compliance with applicable law, HHS Policy, security standards and controls. By using HHS Information Resources, or using, disclosing, creating, transmitting, or maintaining HHS Confidential Information or HHS Agency sensitive information, I consent to the monitoring of the use of these resources and information in any form and on any device and understand I have no expectation of privacy.

[3] http://hhscx.hhsc.texas.gov/it/policies-and-guidelines
[4] http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

Health and Human Services
Acceptable Use Agreement (AUA)
(Formally known as the Computer Use Agreement or CUA)

Non-Compliance

I understand that non-compliance with this agreement or violation of the HHS Enterprise Information Security Acceptable Use Policy (AUP) may be cause for removal of access and disciplinary action, up to and including dismissal and/or civil or criminal prosecution. I also understand that I must comply with applicable law and HHS Agency policies, procedures, standards and guidelines over Information Resources, HHS Confidential Information, and HHS Agency sensitive information such as the requirements in the HHS Human Resources Manual, HHS Privacy Policy and HHS Security Policy, as well as any changes to those requirements.

Depending on the severity of the violation, consequences may include one or more of the following actions:

- Immediate suspension of access privileges and revocation of access to HHS Information Resources, HHS Confidential Information or HHS Agency sensitive information;
- Disciplinary action, up to and including dismissal;
- Removal or debarment from work on HHS contracts or projects;
- Civil monetary penalties; and/or
- Criminal charges that may result in imprisonment for misuse of HHS Information Resources or HHS Confidential Information.

USER MUST ACKNOWLEDGE ALL PAGES OF THIS AGREEMENT.

I have read, understand and agree to comply with this agreement.

HHS Employee Signature: _____

HHS Contractor Signature: _____

HHS Employee/Contractor Name Printed: _____

HHS Employee ID: _____

HHS Agency and Department or Division: _____

Date Agreement Signed _____

Health and Human Services
Acceptable Use Agreement (AUA)
(Formally known as the Computer Use Agreement or CUA)

For the purpose of this document, "HHS", "HHS Agency", or "HHS Agencies" include the Health and Human Services Commission, Department of Aging and Disability Services, Department of Family and Protective Services, Department of State Health Services, Department of Assistive and Rehabilitative Services, and/or any successor agency or component part thereof.

Definitions can be found in the HHS Enterprise Information Security Definitions (http://hhscx.hhsc.texas.gov/it/policies-and-guidelines), HHS Privacy Policies and Procedures and the HHS Human Resources Manual (http://hhscx.hhsc.state.tx.us/hr/HRM/contents.htm).