**Security and Confidentiality Assurance Checklist**

**During the COVID-19 Response**

TB/HIV/STD Section (THSS) security and confidentiality procedures state that confidential records should only be taken to a staff person’s residence during unavoidable circumstances. The supervisor has authority to allow this and must specifically approve it. Removal of confidential records without the supervisor’s knowledge and approval may be subject to disciplinary action. The security and confidentiality of our client’s private health information must be safeguarded at all times.

Given the rapidly evolving nature of the COVID-19 pandemic and the need for the continuity of operations, especially of mission critical tasks such as public health follow-up, confidential records will only be removed from the workspace upon completion and acknowledgement of this checklist. Use and completion of this checklist is required of all THSS staff with the business need to have confidential records in their residence during the COVID-19 modified work approach implemented by DSHS.

|  |  |  |
| --- | --- | --- |
| **Action** | **Staff Initial** |  **Supervisor Initial** |
| **Confidential Information** |
| All applicable security and confidentiality procedures will be followed. The most current security and confidentiality procedures can be found at the [HIV-STD Security Policies and Procedures](https://www.dshs.texas.gov/hivstd/policy/security.shtm).  |  |  |
| Staff will e-mail their immediate supervisor and/or designee of the need to take confidential documents out of the office. |  |  |
| The immediate supervisor and/or designee uses the Section’s check-in and check-out procedure to log the removal and return of confidential information.  |  |  |
| The immediate supervisor and/or designee signature is required at time of check-in and check-out.  |  |  |
| Supervisors and/or designees should ensure the business justification is documented in the e-mail request received.  |  |  |
| Only one week’s work will be taken out of the office at any one time.  |  |  |
| Upon returning to work, confidential information and/or documents should be returned to the office and the supervisor or designee should indicate that the documents have been returned via signature on the check in log. |  |  |
| **Working Out of the Office** |
| Staff will keep their workspace organized and clean.  |  |  |
| Staff will not leave documents unattended or in view of unauthorized people *(this includes family members, roommates, friends, or other individuals).* |  |  |
| Staff will work on confidential information or business-related documents in a private and secure place.  |  |  |
| Staff will keep devices locked when unattended.  |  |  |
| Staff will keep confidential documents locked when not using them to complete a task.  |  |  |
| When participating in video and phone conferences, make sure confidential conversation is private and cannot be heard.  |  |  |
| Staff will not download sensitive or confidential work documents to their work or home computer and/or unauthorized hard drive.  |  |  |
| **IT Security Standards** |
| Staff will ensure that equipment used for teleworking meets all HHS IT security requirements.  |  |  |
| 1. All equipment is configured in accordance with HHS IT standards.
 |  |  |
| 1. All media is encrypted.
 |  |  |
| 1. All security features on equipment are enabled.
 |  |  |
| 1. All automatic operating systems, application security and malware protection updates are enabled.
 |  |  |
| Staff will use only HHS-issued equipment when working with confidential information. *No personal equipment will be used to work or access confidential information.*  |  |  |
| Staff will use HHS VPN prior to logging into HHS systems remotely.  |  |  |
| Staff will only store HHS information on HSS servers. Staff will not store confidential information on their computer’s hard-drive, unauthorized pin drive, or any unauthorized external drives.  |  |  |
| Staff will not use public networks or public machines to log into HHS systems or restricted environments.  |  |  |
| **Transporting of Confidential Information** |
| Staff will transport confidential documents in a secure and locking briefcase or other acceptable container.  |  |  |
| Staff will code to disguise any information that can easily be associated with TB/HIV/STD where possible. |  |  |
| Staff will carry the confidential information in a manner that insures against loss or inadvertent display. |  |  |
| Staff will lock the confidential information in their car’s trunk and out of site from the public when in transport. |  |  |
| Staff will remove the confidential information from their car’s trunk and not leave it in the vehicle during the day or overnight. |  |  |
| **Reporting of Privacy Incidents** |
| Staff will report Privacy Incidents within 24 hours of discovery at [DSHS TB/HIV/STD Section Privacy Incident Report](https://forms.office.com/Pages/ResponsePage.aspx?id=Mnf5m7mCm0mxaqk-jr1Ta8pPRdvSh7ZEjdx2IJWdrCxUN1o0T1hLMUhJWTBEWFVCMERSTVBWRzJMSi4u). *Anyone can report a privacy incident. It is best to let your immediate manager, supervisor, and Local Responsible Party be aware of the suspected incident.*  |  |  |
| Follow-up to the suspected incident will occur and additional forms may need to be completed.  |  |  |

***These are minimum requirements during the response to COVID-19 and can be amended at any time.***

*I attest that I have read and will comply with this Security and Confidentiality Assurance Checklist During the COVID-19 Response and with DSHS TB/HIV/STD Section Policy Number 2016.01, Confidentiality Information Security Procedures Policy. By signing this form, I certify that I understand the above statements and acknowledge that not following these guidelines may lead to disciplinary action.*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Staff Signature Supervisor Signature**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: Date:**