CDETweb Toolbox

User Confidentiality Agreement

CFR45/HIPAA Confidentiality Agreement

You are being asked to sign this agreement because you have requested a user account for CDETweb Toolbox.org

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR Part 160 and Part 164A and C) and other federal and state laws and regulations have been established to protect the confidentiality of personal health information ("PHI"), and provide, generally, that PHI may not be disclosed except as permitted or required by law or unless authorized by the patient.

While The Wistar Institute itself is not directly regulated under the HIPAA Security Rule, it is committed to helping health care professionals and health care institutions with which it collaborates maintain the privacy of their patients' health information. Toward that end, The Wistar Institute has sponsored the development of ***CDETweb Toolbox***, an electronic data management system (EDMS) designed to support compliance with HIPAA and other regulatory mandates by Institute employees and their authorized collaborators or associates at other institutions ("Users").

Please recognize that your use of the CDETweb Toolbox does not relieve you of other compliance obligations that you may have with respect to PHI. For more information on these requirements, Institute employees should contact the Office of Science Administration.

The following sections provide instructions for requesting a CDETweb Toolbox account and specify the data management practices that you, as a User, must adhere to in order to obtain and use your CDETweb Toolbox account.

Requesting an account

To request an account:

1. Print, sign and date this agreement
2. Fill in a request form (available at <<*TBD*>>), have it signed by your supervisor (e.g: Wistar Principal Investigator or the site investigator at a collaborating institution) and submit it to the Translational Research Management Core ("TRMC").
3. With your browser, access https://cdetwebtoolbox.org/ and click on the link "request an account" under the login button.
4. Provide the required information <<online>>
5. The TRMC will confirm your eligibility. This may require TRMC personnel to contact you and/or your supervisor to request further information
6. Once your application is cleared by the TRMC, an account will be created for you

Creating and maintaining a password

1. You will be required to create a new password. Strong passwords are important to restrict the use of your account to you only. In conformance with Wistar policies (https://sharepoint.wistar.upenn.edu/IT/DeptDocs/Standards/Password%20Standards.pdf) your password should:
    a. Contain at least 8 (ideally 12) alphanumeric characters

   b. Contain both upper and lower case letters
   c. Contain at least one number (0-9
   d. Contain at least one special character (such as: !#$%&?@).,
   e. Avoid obvious combinations (e.g.: name + year of birth, first name + last name, wistar1234, etc.)

2. You should never write down your password and store it in a place that is accessible to others (e.g.: post-it note stuck to your computer monitor). If you have to write it down, store it in a locked drawer or offsite.
3. You must never share your login credentials with anyone. Everything you do in CDETweb Toolbox is recorded in an audit trail, and can be directly attributed to you. You are responsible for all of the data that are entered, edited, accessed, retrieved and/or erased from the system under your credentials. Make sure you are held accountable only for YOUR actions.
4. Passwords will automatically expire periodically. Whenever this happens, the system will ask you to create a new one. It is not good practice to cycle between a couple of passwords: you should create a new one each time.
5. If you forget your password, you can reset it using the “Forgot your password?” link at the bottom left of the Login screen. You will be requested to enter your username, and an email will be sent to you with instructions to reset the password. You cannot reuse this email to reset the password again: should you need another reset, send another request.
6. **The TRMC will never ask you for (or provide you with) a password. If you receive such a request, please contact the TRMC Managing Director as soon as possible**

Accessing the system

1. You should access the system exclusively by using your own credentials. You should never have access to CDETweb Toolbox applications or projects that are not under your supervisor’s account. Should you inadvertently be granted access to such applications or projects, you are required to report this occurrence immediately to the TRMC Managing Director.
2. CDETweb Toolbox must be accessed using the web interface provided.
3. Your access to specific tools within the system is defined based on your authority profile.
   a. If you find that you do not have access to tools or functions you need, please alert your supervisor, who can contact the TRMC to rectify the problem.
   b. If you notice that you have access to tools or functions, or in any other way you are exposed through CDETweb to restricted information, to which you should not have access, you should contact the TRMC Managing Director immediately. Remember that any activity performed under your login credential is directly attributable to you, and you will be responsible for any unauthorized entry.
4. Read-only root access to the system database tables can be allowed under very limited circumstances, and must be arranged through the TRMC Managing Director. Wistar IT Department authorization may also be needed.
5. The unauthorized use of unapproved applications, programs and any other electronic means to access the system’s back-end tables is absolutely forbidden.

6. The Institute owns and/or is responsible for all the data stored in CDETweb Toolbox. Any unauthorized access is strictly prohibited by Institute policy, and by relevant state and federal laws.

Entering and editing data

1. All data entry must be executed through the CDETweb Toolbox web application, including bulk data uploads (i.e.: uploads from .csv or excel tables). Any other form of data entry is not authorized.
2. The system allows data entry pages (forms) to exist in multiple modes.
    - a. Once you start entering data in a form, it will automatically switch to “edit” mode. Keep it in edit mode until you are done entering and editing data. The system will save the data but the form will remain open.
    - b. Once you are finished, you should switch the form mode to “lock”. Locked forms are protected from editing, and data can be viewed but not modified.
        - i. Notice that, with some exceptions (for example, some logs), only “locked” data will be displayed in reports, since unlocked data are considered works-in-progress.
    - c. If you need to amend the data and your account setup does not grant you the authority to unlock a form, you should contact your supervisor to determine who has the authority to unlock and amend data for you.
        - i. Once the form is unlocked, you can amend the data and lock the form again. Notice that any data change will prompt a request to indicate the reason for the change, which will be recorded in the audit trail.
        - **ii. Avoid multiple amendments to data. These are tracked and indicate poor data quality. Therefore, do not lock the forms until you are reasonably sure that all the data has been entered correctly.**

Managing data files

The CDETweb Toolbox’s **File Management** tool allows users to upload files to the CDETweb Toolbox hosting server via an https protocol. This guarantees that all data are encrypted in transit.

HIPAA regulations require that PHI stored on servers be encrypted “at rest” (i.e. the information must be encrypted while it resides on the server).

In order to maintain compliance with HIPAA regulations, files containing PHI in any form (including, but not limited to, one or more of the 18 “safe harbor” HIPAA identifiers) must be encrypted with a FIPS-140 compliant cipher (current examples include AES-128 or ideally AES-256) before being uploaded to the server.

Importantly, encryption keys should never be uploaded/transmitted/stored with the file they belong to.

Notes:

1. File uploads should be used to securely exchange information that cannot be captured through CDETweb Toolbox forms. This may include supplemental information or “one-off” query results.

2. File uploads should not be used as a substitute for CDETweb Toolbox forms: to ensure data integrity GCP, GAAMP6 and 21CFR part 11 regulations require the tracking of data through an audit trail. While CDETweb Toolbox maintains a log of the files uploaded, this is not intended to replace the data audit function provided by the tables.
3. *Wistar Employees*: With the exception of “limited data sets”, Institute policies prohibit storage of PHI on your local client hardware (including PCs, notebooks, shared server volumes, cloud storage, cell phones and tablets, USB thumb drives, personal storage devices, etc.).
4. Limited data sets, as defined in http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/, should be stored in accordance with Wistar Institute policies. Please consult with the Wistar Institute IT department to address any topic related to storage of limited data sets outside of CDETweb.

Data safety

1. CDETweb Toolbox handles data in compliance with current regulatory mandates. However, your responsibility is not limited to entering the data in the system. To remain compliant, you must successfully complete training in the following categories:
    a. Human Subject Research
    b. Information Security Awareness

    NOTES:
    - *Training for Wistar Employees is provided through the Office of Science Administration (OSA). Please contact the OSA for details on training modules and access.*
    - *Proof of equivalent training will be required for non-Wistar Employees*
2. The following are strictly prohibited:
    a. CDETweb Toolbox screen printouts, captures, photographs or any other way by which the information displayed in your browser is captured and/or reproduced;
    b. Sharing information with anyone who is not authorized by your supervisor or the TRMC to have access to the system (e.g. screen sharing, credential sharing etc.) and; communicating PHI to any unauthorized individuals by any other means, including by verbal, written or visual means.
    c. Entering information that can be construed as PHI in CDETweb open text fields.

CONFIDENTIALITY STATEMENT

As a CDETweb Toolbox user, I understand that I may be working with PHI.

I acknowledge that it is my responsibility to respect the privacy and confidentiality of PHI and other confidential information. I will not access, use or disclose such information unless I do so in the course and scope of fulfilling my employment duties.

I understand that I am required to immediately report any unauthorized access, use or disclosure of PHI to my supervisor or the TRMC.

I understand and acknowledge that my failure to comply with any provision listed in this agreement may result in the suspension or termination of my access privileges to CDETweb Toolbox, as well as civil or criminal liability under federal or state law, and/or disciplinary action under my employer's applicable policies, up to and including termination. Violations of this User Confidentiality Agreement will be communicated to my supervisor/employer by the TRMC.

Signature	Printed Name	Lab/Department	Supervisor/PI	Date

HIPAA

- 45 CFR Part 160 and Subparts A and C of Part 164

Appendix 1: Relevant Wistar Policies and Standards

- Wistar Information Technology Acceptable Use Policy
- Wistar Information Security Policy
- Wistar Password Standard
- Wistar - Receipt and Use of Data and Biological Specimens from Organizations that are Covered Entities Under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) – to be issued Oct 2015
- Wistar - Policy Concerning Data Breaches Involving Research Data – to be issued Oct 2015
- Wistar - Provision of Subject-Level Research Data and Biospecimens to Third Parties for Secondary Research Uses – to be issued Oct 2015

Appendix 2: CDETweb Toolbox account request form

Please complete this form and submit it to the Translational Research Management Core to request an account on CDETweb Toolbox.

NOTE TO USERS
By signing and submitting this form you agree to the terms of use detailed in the CDETweb Toolbox User Confidentiality Agreement (UCA). Failure to abide by this UCA may result in the suspension or termination of your access privileges to CDETweb Toolbox, as well as civil or criminal liability under federal or state law, and/or disciplinary action under your employer's applicable policies, up to and including termination.

1. User Name			
First			
Middle			
Last			
2. Email address			
3a. Wistar Employees			
Employee number			
Laboratory / Dept.			
3b. Other users			
Employer's name			
Address			
4. Principal Investigator / Supervisor			
Project(s)			
5. IRB protocol/exemption associated with project(s)			
Protocol/exemption number(s)			
Expiration Date			
6. PI/Supervisor signature [1]		7. Date	
8. User Signature [2]		9. Date	

1. By signing this form the PI/Supervisor attests that:

   a. The User requesting the account has received all appropriate training as verified by Wistar Office of Science Administration.

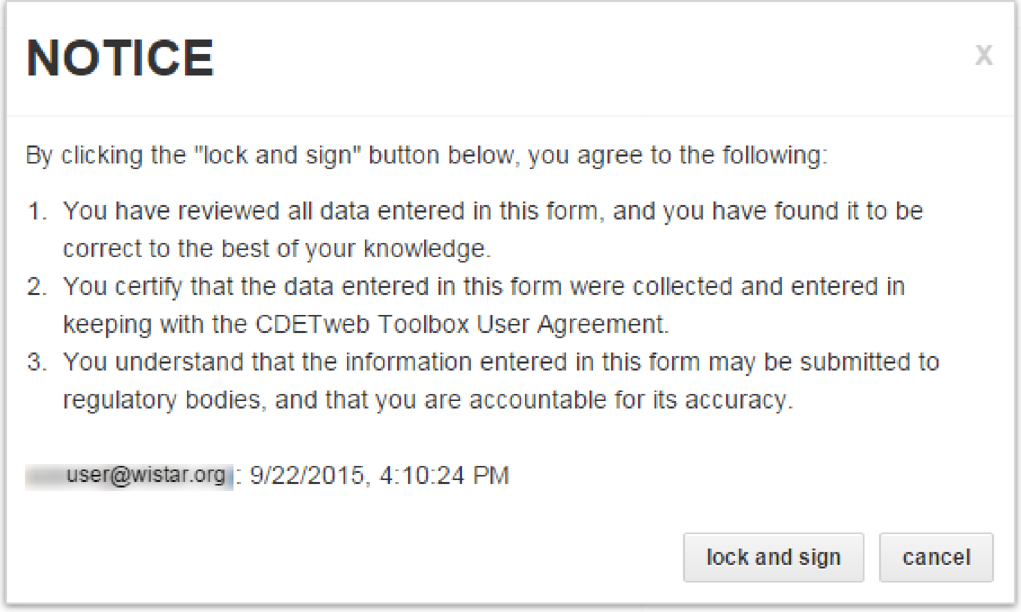
   b. The Project(s) listed above is associated with an active IRB protocol or IRB exemption

   c. If the User's association with your Project/Laboratory is terminated, you will immediately alert the TRMC facility and request that his/her account be inactivated

2. By signing this form the User agrees to the terms of use detailed in the CDETweb Toolbox User Confidentiality Agreement

Appendix 3: Electronic signature language

The following message will be displayed in CDETweb Toolbox when a user locks a form:



NOTICE

By clicking the "lock and sign" button below, you agree to the following:

1. You have reviewed all data entered in this form, and you have found it to be correct to the best of your knowledge.
2. You certify that the data entered in this form were collected and entered in keeping with the CDETweb Toolbox User Agreement.
3. You understand that the information entered in this form may be submitted to regulatory bodies, and that you are accountable for its accuracy.

[redacted]user@wistar.org : 9/22/2015, 4:10:24 PM