Maryland Department of Health and Mental Hygiene
Center for Cancer Surveillance and Control
Surveillance and Evaluation Unit
Cancer Prevention, Education, Screening and Treatment Program

CPEST Client Database (CDB) Policy and Procedures

April 2006; Revised February 2011

Table of Contents

CPEST Client Database (CDB) Policy and Procedures

Introduction

The Center for Cancer Surveillance and Control (CCSC), Maryland Department of Health and Mental Hygiene (DHMH) has developed the Cancer Client Database (CDB). CCSC contracted with University of Maryland, Baltimore (UMB) for the development and implementation of the CDB. The CDB was created by Ciber, Inc. as a data collection tool for local health programs receiving Cigarette Restitution Fund Program, Cancer Prevention, Education, Screening and Treatment Program (CRFP/CPEST) funds in order for local health programs to fulfill reporting requirements.

This document outlines information about the CDB and its use. It also provides the policy and procedures that will assure confidentiality, integrity, and availability of client information. This document provides users with minimum standards and guidance for the handling and security of CDB information.

Policy

Local agencies and DHMH shall ensure confidentiality of CRFP/CPEST CDB data and shall protect the CDB system and its data against unauthorized access or use.

Description of CDB

The CDB is a confidential client database developed under the CRFP to capture information regarding screening, diagnosis, and treatment for selected targeted cancers. The CDB is currently designed to capture specific information on colorectal, oral, prostate, and skin cancers. Users of the database consist of personnel from local health departments, academic health centers in Baltimore City, and DHMH. For security reasons, each user must be approved as a user by the person's supervisor and by the CCSC staff, and must be assigned access to functions of the CDB appropriate to that user as identified by the person's supervisor and implemented by the CCSC staff.

The CDB is a Web-based application for the CCSC unit deployed within the DHMH Internet. The application is accessed using a Web browser, such as Internet Explorer, and is written in Cold Fusion, Microsoft SQL, and Crystal Reports. The system is presently configured to handle at least 1,000 concurrent users who add and update client screening, diagnosis, and treatment data, and can be scaled up to manage a greater load. Since the information in this system is confidential, numerous security measures have been designed into the architecture.

Recommended Operating Environment

Software/Hardware	Minimum	Ideal
Internet Explorer	Version 6	Version 6 or later
Adobe Acrobat Reader	Version 5	Version X (most recent)
Microsoft Word	2000	2000 or later
Microsoft Excel	2000	2000 or later
Operating System*	Microsoft XP	Microsoft XP or later
PC processor	1 GHz	1 GHz or higher

*** Windows 98 and other operating systems below version Windows 2000 are not supported.

CDB Considerations

Training Requirement for CDB Users

CCSC offers two levels of classes to new users of the CDB:

1. Introduction to CDB.
2. Advanced CDB Features.

Introductory training class is mandatory for all users. If a user cannot attend a class by DHMH, please inform CCSC so that alternative training arrangements can be explored. For registration and class schedule, contact the CCSC Surveillance and Evaluation Unit at 410-767-0791.

Access to the Database

To gain access to the CDB, a potential user must complete and the supervisor sign the Database Access Request Form, the Confidentiality Statement, and the DHMH Acknowledgement Form as described in CCSC Health Officer Memo #11-08 (or as subsequently updated). Once CCSC receives the completed, signed forms, CCSC will create the user ID and temporary password and will notify the user of the account information and need to change the temporary password. In order for the user to obtain the information, the user must call a CCSC CDB System Administrator who will then, as a security measure, immediately call the user back to confirm access and provide login credentials. The system will automatically inactivate user accounts that

have not been accessed in 60 days. Users who are locked out will have to submit a request to have the account reactivated if needed.

Use of Client Data Outside of the Office

The user must comply with the DHMH data Confidentiality Agreement that is signed when obtaining the CDB user account. The CDB shall not be used in a public place or on a public computer and shall be accessed at a worksite approved by the user's supervisor. Use of computers and of confidential data from the CDB outside of the office (such as in the home of a teleworking user) must be handled with the same security and precautionary measures as those implemented within the office. All recommendations listed below in section "Procedures to Protect Data" must be implemented.

Use of Laptops

Because of security concerns, the use of laptops for accessing the CDB should be handled with extreme care and precautions. All recommendations listed in section "Procedures to Protect Data" must be implemented on the prescribed laptop and DHMH Laptop Protocol must be adhered to when using laptops; CCSC recommends additionally that confidential data ***not*** *be stored on laptops or on removable media, such as flash drives or DVDs unless* the data can be adequately secured, both physically and electronically using a DHMH-approved encryption scheme.

Procedures to Protect Data

Below are measures for safeguarding client information and system access. These measures are required in addition to other procedures that are already in place at your location.

Feature	Recommended Steps
1. Confidentiality of client records in CDB	**All client information in the CDB is confidential medical information** and is protected to the full extent of Maryland and Federal law (HIPAA, Health Insurance Portability and Accountability Act). *Follow your Health Department/Program guidelines for handling confidential medical information. *Use information resources (including data, records, documentation, and database) only for intended purposes according to State policies, laws, and regulations.
2. Access by the user and termination of access	*Notify DHMH in writing to request authorization for system access. *Notify DHMH in writing within one day when an employee or contract personnel with system access is terminated or will no longer require access to the system. Note: system will automatically terminate a user after a period of 60 days of inactivity. *Maintain accurate and up-to-date role assignments in the system

	for staff so that the system access granted by user roles is appropriate for each user. Once a user has been granted access to the CDB with an assigned user role that has certain rights, the user ID, password, and access to the CDB are for that user only and are not to be shared to allow any other person to gain access. *__Do not share your CDB login user name/ID, password, access, or proprietary information with anyone else.__
3. Screen saver on your computer display that is password protected	__*__Go to Control Panel and then Display __*Set your display screen saver__ to activate in 10 minutes if you make no keystroke. Set __"On resume, password protect"__ so that the user will have to enter the password to gain access after 10 minutes. *Protect system access by logging out of the CDB when leaving the computer for more than a brief period of time.
4. Password	__*Never tell anyone your password.__ __*__Keep your password secure and do not display it in a place where someone could easily find it. *To create passwords, use 8 - 10 alphanumeric characters, mixing numbers, symbols, and letters. Your Internet Browser may ask if you wish it to remember your password for this application. __Say "NO." You should enter your password each time you enter the CDB application.__
5. Back/Forward Button on Web browser	__DO NOT__ use the browser's Back and Forward Buttons; rather, use the Previous and Next buttons and the Go To button. While the browser buttons may work in some instances, they are not designed for use with the application. Information entered in the database is __not saved__ if the browser buttons are used so the user may lose work.
6. Temporary Files	Temporary files are created that may contain sensitive information. *Delete these files by following these instructions: 1. Open your Internet Explorer Browser. 2. Click on Tools from the main menu (top of the screen). 3. Click on Internet Options and then click on Advanced tab. 4. Scroll down to the bottom of the list of features and put a check mark in *Empty Temporary Internet Files Folder when Browser is Closed (if not already checked).* 5. Click Apply.
7. Physical Security	• Lock up printed confidential information. • Shred unwanted information using a cross cutting shredder.
8. Confidential Folder	Create a Confidential Folder on your computer where you may save files with confidential information in one location. Purge unneeded files often.
9. Web address of the CDB	*Users may store the Web address of the CDB in their favorites or their Favorite Bar in their Internet Browser. *CCSC recommends NOT putting a shortcut to the CDB on the user's desktop.

Applicable DHMH Policies

Below are policies mandated by the Department of Health and Mental Hygiene:

1. DHMH Electronic Information System Policy 02.01.01
   http://www.dhmh.state.md.us/policies/020101.pdf

2. DHMH Software Policy 02.01.02
   http://www.dhmh.state.md.us/policies/p020102.htm

3. DHMH Information Assurance Policy 02.01.06
   http://www.dhmh.state.md.us/policies/summary.htm

4. DHMH Policy 02.09.11-Policy for Education, Training and Awareness of the Health Insurance Portability and Accountability Act (HIPAA)
   http://www.dhmh.state.md.us/policies/pdf/020911.pdf

5. DHMH Laptop Protocol
   http://dhmh.maryland.gov/policies/laptop.htm

Salient Features of DHMH Policies

The main purpose of DHMH policies is to assure confidentiality, integrity, and availability of DHMH information assets. Following are salient features of these policies:

Ethical Use

All users of DHMH information systems are required to use the electronic information systems in an efficient, ethical, and lawful manner.

CDB System Users must abstain from illegal, unethical, or other prohibited use of DHMH data and systems. These include fraudulent, harassing, threatening, discriminatory, racist, hate-based, lewd, sexually explicit or otherwise disruptive communication and use of data.

Consequences of Violation

Upon discovery of a possible violation of DHMH policies and guidelines, user's access to computer and related information systems may be suspended immediately. In addition, personnel actions up to and including termination may result.

Ownership

All information, in any format, which is created or used in support of DHMH business, is to be considered either owned by DHMH or in DHMH custody. This information is a valuable asset

and must be protected from its point of origin through its life cycle of creation, collection, maintenance, authorized sharing, and storage, until its lawful disposal. It is to be maintained in accordance with federal and State regulations and DHMH policies in a secure and reliable manner. Such protection levels are to reasonably assure confidentiality, integrity, accuracy, and ready availability for authorized use.

Encryption Methods

Users shall not use encryption methods that disguise a prohibited use without formal permission. Only authorized encryption methods provided by DHMH can be utilized.

Deletion of Files

Be aware that deleting files does not constitute complete confidentiality of files. Certain DHMH procedures retain data. You are discouraged from saving confidential data on your computer. However, if you have to save records, save them in an inconspicuous folder and delete them after they have been used.

Password Protection

Users are responsible for protecting their own password. Sharing or posting of CDB or EDB user IDs, passwords, VPN (crypto card, Pin Number) is not permitted. If emergency access is required, this information should be disclosed to a system administrator or facility administration.

Damage to Systems

Deliberate use of software (virus) to damage, destroy, corrupt, or impede DHMH information systems is grounds for termination of employment. Employees are required to use authorized computer virus detection software provided by the administration.

Any activity that would damage the Department's reputation or potentially place the employee and DHMH at risk for legal proceedings by any party is prohibited.

Access Level

Based on a "need-to-know" approach, supervisors are to assign employees an appropriate access authority and grant corresponding system access levels.

Secure Access

Work may not be performed away from the worksite unless all prevailing and appropriate security and confidentiality policies and laws are strictly adhered to. In addition, this policy prohibits direct dial-up access to the network or simultaneous dial-up and network connections to

those instances where pre-approved alternatives are not available. The exceptions are for the use of GroupWise or other approved e-mail systems.

Actions that may reasonably be construed as hostile by another organization, institution, or individual (internal or external to DHMH) are prohibited. An example of this is attempting to gain unauthorized access to another computer system or information.

Software Copyright

All employees of the DHMH are told that they shall not make copies of software products or software documentation or use office computers for any purpose other than official business. Software not specifically purchased or acquired through established procurement channels is not authorized for use on DHMH computers. Freeware and/or Shareware products must be reviewed by the Information Technology Support Division before they can be used on any DHMH personal computer (PC), regardless of whether the PC is networked or not. All employees are told that they must sign the State of Maryland Software Code of Ethics.

Personal copies of legally licensed software may be used for business purposes if all of the following conditions are satisfied: 1) The State Software Policy is observed, 2) The license is transferred to DHMH, 3) The supervisor provides written approval, and, 4) The software is installed on State equipment by the authorized system administrator.

Supporting Documents

Tips for CDB Use
Client Database User Guide
Client Database Training Manual

****

Please call CDBHelp at 410-767-0791 for assistance or e-mail CDBHelp@dhmh.state.md.us

****