TIMS

Tuberculosis Information Management System

User's Guide

April 2003

Version 1.2

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Public Health Service

Centers for Disease Control and Prevention

National Center for HIV/STD/TB Prevention

Division of Tuberculosis Elimination

Introduction

Introducing TIMS

Welcome to the Tuberculosis Information Management System, or TIMS. This User's Guide will provide the information you need to operate the TIMS application successfully.

TIMS is designed for the Microsoft® Windows® operating environment and will work with all versions of Windows 95®, Windows 98®, Windows NT® 4.0 or Windows 2000®.

TIMS has two key objectives:

1. To provide tools that will aid healthcare facilities in their effort to treat, control, and eliminate tuberculosis in the United States and its outlying territories.

2. To gather tuberculosis surveillance information so that it can be transmitted to the Centers for Disease Control and Prevention (CDC) for statistical and research purposes.

TIMS Features

Here are some of the key features of TIMS:

- Combines functions of TB surveillance and patient management into one application
- Supports electronic reporting of TB surveillance data
- Provides a windows-based Graphical User Interface
- Supports either standalone or LAN-based multi-user operation
- Enables you to export data to other applications
- Minimizes data re-entry by allowing sharing of data between modules

System Requirements

TIMS requires the following minimum system configuration:

- Personal computer 486/66 or higher processor (Pentium recommended)
- 16 megabytes (MB) of RAM (32 MB or more recommended)
- 50 MB of free hard disk space
- Microsoft Windows 95, Windows 98, Windows NT 4.0 or Windows 2000
- Windows-compatible mouse
- 9600 baud modem
- Dedicated dual-standard phone line

TIMS can be installed for multi-user operation on a local area network (LAN) on the following network operating systems:

- Novell® NetWare® version 3.1 and later
- Microsoft Windows NT Server 4.0 and later
- Microsoft Windows 2000 Server

TIMS Modules

TIMS functions are divided into modules to promote flexibility and ease-of-use. While all modules are available to all users, the functions available within those modules depend on the user privileges assigned by your TIMS system administrator. Some functions are disabled completely or have restricted capabilities for some users. See the System Module chapter in this manual for additional security-related information.

The modules are:

- Client
- Surveillance
- Patient Management
- Daily Program Operation
- Program Evaluation
- System

Client Module

Use the Client module to create, retrieve, and maintain client specific identification and demographic information. This is a client-centered module.

Surveillance Module

Use the Surveillance module to record and report client tuberculosis information to the proper public health authorities. The Surveillance module contains electronic duplicates of three related documents:

- Report of Verified Case of Tuberculosis (RVCT)
- Initial Drug Susceptibility Report (Follow Up-1)
- Case Completion Report (Follow Up-2)

This is a client-centered module.

Patient Management Module

Use the Patient Management module to track clients' medical treatment, contacts, and tests.

Information entered in the Patient Management module can be imported into documents in the Surveillance module. See the Surveillance Module chapter in this manual for additional information about generating data.

This is a client-centered module.

Daily Program Operation Module

Use the Daily Program Operation module to record information about your facility. Daily Program Operation records information about your staff (appointments, languages spoken, etc.) and other operations-related features.

Program Evaluation Module

Use the Program Evaluation module to create, maintain and transfer Aggregate Reports for Program Evaluation (ARPE).

System Module

Use the System module to maintain the TIMS software installation and manage your data. The System module allows you to:

- Add and remove TIMS users
- Change your password
- Transmit surveillance data to the proper public health authorities
- Set Preferences
- Create Ad Hoc Queries and Frequency Reports
- Export data to other applications

The System module also provides a number of other options that allow you to ensure that TIMS runs smoothly and records data accurately. Most of the functions in the System module are restricted to High or System Administrator access privileges.

Using TIMS Documentation

TIMS User's Guide

The TIMS User's Guide contains a series of chapters and appendices that provide a complete reference to the TIMS application.

Chapter 1 - The *TIMS Workplace.* Describes and illustrates the TIMS user interface.

Chapter 2 - The *Client Module.* Provides information about adding, editing, and maintaining basic information (such as name, address, and social security number) for each client.

Chapter 3 - The *Patient Management Module.* Provides information about adding, editing, and maintaining tuberculosis-related information about specific clients. Includes information on storing diagnoses, medication, test results, and other TB-related data.

Chapter 4 - The *Surveillance Module.* Provides information about adding, editing, transferring and maintaining Report of Verified Case of Tuberculosis (RVCT) data.

Chapter 5 - The *Program Evaluation Module.* Provides information about creating, maintaining and transferring Aggregate Reports for Program Evaluation (ARPE).

Chapter 6 - The *Daily Program Operation Module.* Provides information about adding, editing, and maintaining information about your site, including workers providing services to clients.

Chapter 7 - The *System Module.* Provides information about performing system-related functions in TIMS: maintaining TIMS tables, transmitting data, adding and deleting TIMS users, querying data, etc.

Surveillance Appendices. Provide specific guidance, including definitions and coding tables for use in collecting and entering RVCT data.

Program Evaluation Appendix. Provides specific guidance, including definitions and coding tables for use in collecting and entering Aggregate Reports for Tuberculosis Program Evaluation (ARPE).

Patient Management Appendix. Provides forms for use when collecting patient management data from clients.

Reports Appendices. Provide definitions and samples of all Surveillance and Patient Management module reports.

System Appendix. Provides system security information for all modules within TIMS.

User's Guide Conventions

Understanding the conventions employed in the User's Guide can help you use it more effectively.

Whenever possible, the TIMS procedures are divided into numbered steps. Follow the steps in order to complete the task.
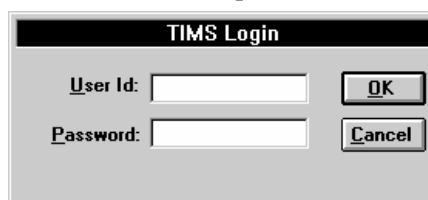
Example

Type your User ID in the **User ID** field.

> User IDs are assigned by a TIMS System Administrator. The User ID must be entered exactly as it was given to you.

Type your password in the **Password** field.

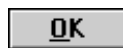> Passwords are not case-sensitive: PASSWORD = password = PassWord

Click the **OK** button.

> **Bold** type is used to identify program controls such as buttons, menu items, text boxes, etc.

Example

1. Click the **OK** button.

Online Help

TIMS includes integrated, context-sensitive online help. Use the online help system to get information while operating the TIMS application, or you can view the help independently by opening the TIMS.HLP file (located in the TIMS program directory on your local hard drive or Local Area Network (LAN) server.
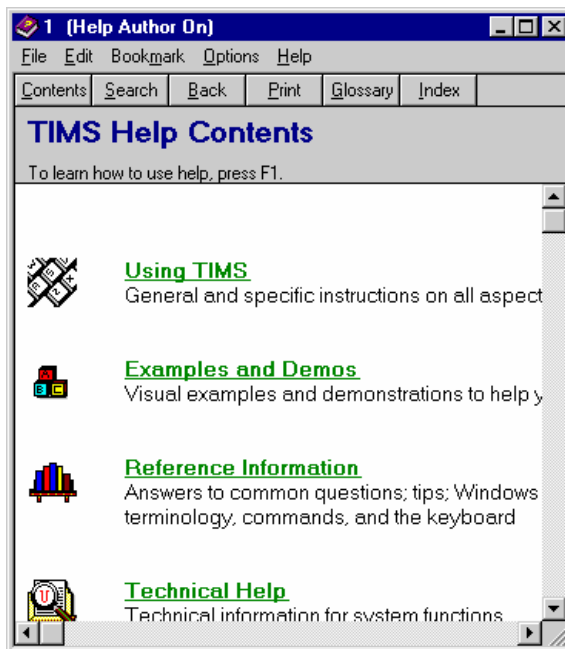
See Chapter 1 - The TIMS Workplace for additional information about TIMS online help.

Service and Support

Phone Support

If you experience problems with TIMS that you cannot resolve, please contact the TIMS Help Desk at (770) 234-6500. The TIMS Support Team is available Monday through Friday, 8:30 a.m. to 4:30 p.m., Eastern Time.

E-Mail Support

If you prefer, please e-mail questions and comments to the TIMS Support Team. The e-mail address is **timshelp@cdc.gov**.

Confidentiality, Data Security, Data Integrity, and Dissemination of Data

The Division of TB Elimination in the National Center for HIV, STD and TB Prevention has obtained from the Director of the Centers for Disease Control and Prevention (CDC) an Assurance of Confidentiality to protect the CDC expanded TB surveillance system. State and local TB control programs should ensure that their policies and procedures protect the confidentiality of their TB surveillance systems. Policies or procedures should be in place to protect all TB reports, records, and files containing patient names and other identifying information. Local policies regarding the confidentiality of such information, especially HIV test results, should adhere to all applicable state and local laws. These protections should include the use of TIMS software and databases.

Protecting the Confidentiality of Data Collection Forms, Reports, and other Patient Information in the TB Surveillance Program

1. All Report of Verified Case of Tuberculosis (RVCT) forms, communicable disease report cards, computer media, or other records which contain patient names and other identifying information should be kept in closed, locked files except when being processed by TB surveillance staff. Offices should be locked during non-business hours. No papers should be exposed when the employee is away from the work area, even for brief periods. Hard copies of RVCT forms, communicable disease report cards, and other records should be retained as required by state or local communicable disease laws and other applicable laws or regulations.

2. Access to all RVCT forms, communicable disease report cards, and the files containing them should be restricted to designated TB surveillance staff who are directly involved with surveillance and other case work, and who have a need to know.

3. **RVCT forms should never be mailed to CDC**. All TB surveillance records are reported to CDC via modem or email (in an encrypted format) using CDC's Tuberculosis Information Management System (TIMS) software. Although TIMS allows for the collection and storage of personal identifiers such as names and street addresses for local and state TB surveillance purposes, **these identifiers are not transmitted to CDC**. In general, any surveillance information sent through the mail should be stamped "confidential," should be addressed to a specific person (or sent to that person's attention), and should be sent by secure mail. These precautions will help to limit the possibility of unauthorized access to surveillance information.

Warning: Unauthorized use of this system is prohibited by Title 18 of the United States Code. Reverse engineering, deciphering, or any other attempt to produce non-executable forms of this program is not authorized and may be prohibited by federal and state laws. In addition, this software may process data protected by other federal and state laws. Information regarding unauthorized use of this software or access to protected data will be referred to the Federal Bureau of Investigation and the United States Department of Justice for prosecution.

Protecting the Confidentiality of Records and Reports in TIMS

1. Access to all electronic surveillance data (e.g., TIMS, TB registers, backup media, and other surveillance databases) should be restricted to designated TB surveillance staff who are directly involved with surveillance and other case work, and who have a need to know.

2. Access to TIMS is protected by a user ID and password combination. Password creation and administration should adhere to the following guidelines:

   • User IDs must be issued by the TIMS Administrator and should be issued only to designated members of the surveillance staff who require access to TIMS to perform their official duties.

   • The master administrator password for the TIMS application should be updated and changed on, at least, a quarterly basis.

- User passwords should be changed on, at least, a quarterly basis.

- Passwords should not be easy to deduce (e.g., staff members' names, birthdates, or other unique information that might be "guessed" by an unauthorized person trying to access confidential files). Ideally, it should contain both numbers and letters.

- User IDs and passwords should never be shared between individuals.

- User IDs belonging to individuals who are no longer authorized to access TIMS must be immediately deleted or made inactive by the Administrator.

3. All computers or workstations accessing TIMS, performing analyses on data or files exported from TIMS, or other surveillance databases must be kept in a restricted or locked area. Users should solicit the assistance of their IT support staff to protect both physical and electronic access to a TIMS workstation and its related confidential data. CDC recommends the utilization of workstation and network options that result in a workstation lock after a specified idle period of time. Refer to the User's Guide supplied with the computer for information on the security options available.

4. All confidential hardcopy output (e.g., file listings, reports, etc.) generated by TIMS or other surveillance databases must be kept in a restricted or locked area. All hardcopy output that is no longer needed must be destroyed.

Protecting the Security of Records and Reports in TIMS

1. All computers and workstations accessing TIMS should be protected from electronic viral contamination. Shareware or other programs or files of unknown origin should never be installed on the computer. Diskettes or other external media of unknown or questionable history should be formatted prior to use. Damaged media should be destroyed. CDC recommends that each site make appropriate use of up to date anti-virus software including explicitly turning on features that allow for boot sector, email, file, and workstation scanning and virus signature updates on a set schedule.

2. To enhance security, information in the TIMS database is not accessible to any other application without appropriate user id and password.

3. Additional security measures (e.g., restricted access to the PC, locating the PC in a secured area, etc.) will further protect patient confidentiality and data security. All TIMS administrators should review their security system as soon as possible to determine whether it is adequate. The TIMS administrator should conduct periodic reviews or audits to ensure compliance with all data security procedures.

4. Where TIMS is installed in a network environment, it is recommended that standardized network operating system file and user account permissions be utilized appropriately to prevent non-TIMS users from gaining access to TIMS application and/or data directories.

5. Client-related information is encrypted before it is transmitted to other TIMS sites and is not decrypted until it is processed in the TIMS InBox at the receiving site. Transmission acknowledgements do not contain confidential information and are not encrypted.

6. The National Electronic Telecommunication System for Surveillance (NETSS) files, which are also created by a TIMS Data Transfer process, do not contain confidential patient identifiers and are not encrypted. The NETSS files are created in the Surveillance module and the destination of the output is configured in the System module. See the appropriate chapters in the TIMS User's Guide for details.

7. Files exported from TIMS are not covered by CDC's Assurance of Confidentiality (page xiv). Such exported files may contain confidential patient information, and must be protected as such.

Protecting the Integrity of Databases in TIMS

1. Key entry of data and/or the use of the TIMS Import Utility are the only authorized methods to enter data into TIMS. Data from other sources (e.g., mainframes or other surveillance databases) must not be imported into the TIMS databases (except via the use of the TIMS Import Utility). Such unauthorized attempts to load data into TIMS jeopardizes the integrity of local, state, and national TB surveillance data.

2. To create database copies for external analysis, the user must use the Database Export, Adhoc Query, or Flat File Export features found on the **Data Mgt** menu in the System module. Copies of the TIMS databases or data exported from TIMS cannot be imported back into TIMS, except via the TIMS Import Utility.

3. To protect the integrity of the database, the restore function available in TIMS can only be executed with a password provided by the CDC. All sites must coordinate with CDC should it be necessary to restore the database from a TIMS backup copy or a LAN backup. Call the TIMS Help Desk at (770) 234-6500 prior to restoring a database to receive a password and to ensure that appropriate procedures have been implemented to assure data integrity.

Assurance of Confidentiality for
Reports of Verified Cases of Tuberculosis (RVCT),
Centers for Disease Control and Prevention (CDC)
Control Number M3-91-027

Reports of Verified Cases of TB (RVCT) are submitted to CDC from TB control programs in all states, most large cities, and U.S. Territories and Commonwealths. The surveillance information requested by CDC consists of detailed reports of persons with TB, including information on the individual's HIV serostatus, demographics (e.g., homelessness, correctional institution, or long-term care facility), alcohol and drug use, drug therapy, and drug susceptibility results. The data are used by U.S. Public Health Service scientists and cooperating state and local health officials to help understand and control the spread of TB.

Information that would permit identification of any individual on whom a record is maintained by CDC is collected with a guarantee to the agency, institution, physician, or individual providing the information that it will be held in strict confidence, will be used only for purposes stated in this assurance, and will not otherwise be disclosed or released without the consent of the individual in accordance with Sections 306 and 308(d) of the Public Health Service Act (42 U.S.C. 242k and 242m(d)). Data or information retained by the state or local health officials or by authorized collaborating researchers will be protected in accordance with state law.

Information reported to CDC will be used without identifiers for statistical and analytic summaries in which no individual on whom a record is maintained can be identified and for special studies of the transmission, natural history, and epidemiology of TB associated with HIV infection. When necessary for confirming information, or in the interest of public health and disease prevention, CDC may confirm information contained in case reports or may notify other medical personnel or health officials of such information. In each instance, only the minimum information necessary will be disclosed.

Collaborative research efforts with an important public health purpose will require approval by the Director of CDC pursuant to strict conditions. If disclosure of identifying information to the collaborating researchers is essential to conduct the research, a written certificate will be required that identifying information obtained from CDC will be managed as confidential and will not be released or re-disclosed. No information that could be used to identify any individual on whom a record is maintained, whether directly or indirectly, will be made available to anyone for non-public health purposes. In particular, such information will not be disclosed to the public, parties involved in civil, criminal, or administrative litigation, or non-health agencies of the federal, state, or local government.