

TIMS

Tuberculosis Information Management System

User's Guide

February 2001

Version 1.10

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

All sample information presented in this manual is used for demonstration purposes only and bears no resemblance to actual persons living or dead.

Microsoft, Windows, Windows 95/98, and Windows NT are either trademarks or registered trademarks of Microsoft Corporation. Novell and NetWare are trademarks of Novell Incorporated. Other brands and their products are trademarks or registered trademarks of their respective companies.

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® or Windows NT® 4.0.

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 the functions of SURVS-TB (for surveillance data) and TBDS (for patient management functions) into one application
- Fulfills tuberculosis reporting obligations
- Windows-based Graphical User Interface
- Standalone or LAN-based multi-user operation
- Easy to use
- Enables you to export data to other applications
- Can share data between modules to minimize data re-entry

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 (disk space requirements will be considerable higher if you plan to convert a large SURVS-TB database)
- Microsoft Windows 95, Windows 98 or Windows NT 4.0
- Windows-compatible mouse
- 9600 baud modem (28800 baud recommended)
- 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

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 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)

Completing and transmitting data from the Surveillance module fulfills your tuberculosis-reporting obligation.

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 health authorities
- Change the way some information on the on-screen forms appears

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 is 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) about the people who visit your facility to receive tuberculosis-related services.

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, and maintaining surveillance data that will eventually be transmitted to the CDC.

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 databases, transmitting data, adding and deleting TIMS users, etc.

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.

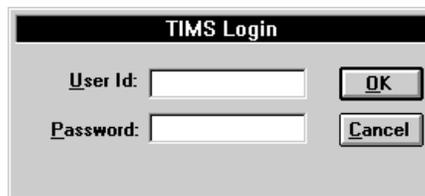
Example

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.

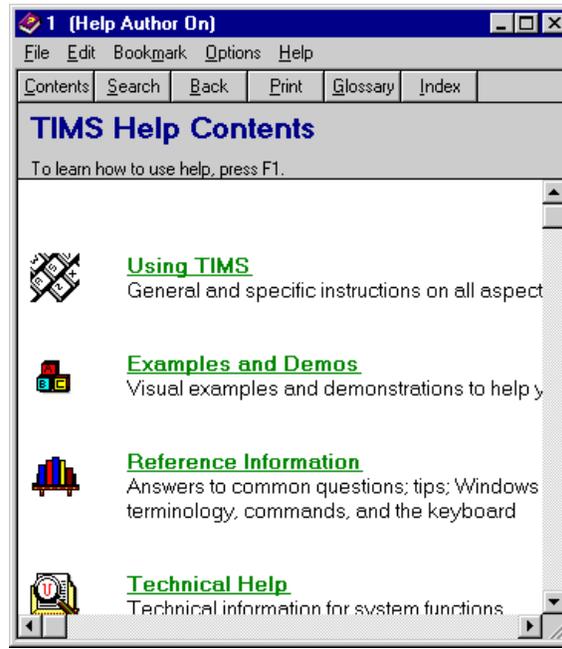
Example

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 (404) 639-8155. The TIMS Support Team is available Monday through Friday, 8:30 a.m. to 4:30 p.m., Eastern time.

E-Mail Support

In addition to phone support, you can 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, 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 (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.
4. The Advisory Council for the Elimination of TB (ACET), recommended at its January 1993 meeting that surveillance information which is necessary to conduct both TB and HIV/AIDS surveillance activities, and is necessary to allow for adequate investigation of TB and HIV/AIDS cases, should be shared between TB and HIV/AIDS surveillance programs within the same health department. ACET also recommended that TB surveillance programs and staff adhere to the same confidentiality standards as HIV/AIDS surveillance programs. TB program staff should work with local HIV/AIDS programs to establish equivalent data confidentiality systems.
5. ACET further recommended that sharing information on HIV serostatus with persons outside the HIV/AIDS and TB surveillance programs of the same health department should only be done with the informed consent of the patient, except in clear emergency situations. For clinical care purposes, HIV-related information should be shared between TB care providers and other health care providers in accordance with state and local laws.

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, and other surveillance databases, etc.) 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. 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. Passwords should be changed on a monthly basis, and 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). 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 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. If this is not feasible, the hard disk must be physically or electronically locked when the computer is not in use. Refer to the User's Guide supplied with the computer for information on the security options available.
4. All 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 of unknown or questionable history should be formatted prior to use. Damaged diskettes should be destroyed. CDC recommends that each site purchases anti-viral software and use it to scan each diskette received from another site. The hard disk should also be scanned periodically for viruses.

Note: All diskettes received by CDC are scanned for viruses.

2. To enhance security, information in the TIMS database is not accessible to any other application at any time.
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.
3. 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.
4. 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.
5. Files exported from TIMS are not covered by CDC's Assurance of Confidentiality (page xv). 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 is the only authorized method to enter data into TIMS. Data from other sources (e.g., mainframes or other surveillance databases) must not be imported, downloaded, or uploaded into the TIMS databases. 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 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.
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 (404) 639-8155 prior to restoring a database to receive a password and to ensure that appropriate procedures have been implemented to assure data integrity.

Dissemination of Surveillance Data

The following recommendations are based on the U.S. Department of Health and Human Services, CDC Staff Manual on Confidentiality (February 1984). Only designated staff members should be authorized to release information to the public. In addition, TB surveillance programs should adhere to all state and local confidentiality laws.

Procedures for Responding to Queries from Persons Outside the Local TB Surveillance Program

1. TB surveillance staff should use discretion and should not discuss sensitive program or patient issues, or records with anyone other than those directly involved in surveillance activities.
2. TB surveillance staff should never reveal the name of a patient or other individual to anyone other than those directly involved in surveillance activities and who have a need to know.
3. TB surveillance staff should never confirm or deny that a particular individual has been reported as having a specific disease or condition to anyone other than those directly involved in surveillance activities and who have a need to know.

Procedures for Releasing TB Surveillance Information

1. All statistical data released by TB surveillance staff should be carefully scrutinized so that individuals cannot be identified. Statistics released to the public should not include any information that would make it possible for a particular individual to be identified. Only designated staff members should be authorized to release information to the public.
2. Line-by-line records from the active TB surveillance databases should not be released for research, or for any other purpose to individuals outside the health department. A separate research database, which groups data as described below, should be created for such release. Alternatively, tables of interest should be produced by surveillance program personnel and only released to outside investigators if the tables meet the following guidelines:
 - A. In no table should all cases of any line or column be found in a single cell.
 - B. In no instance should the total figure for a line or column of a cross-tabulation be less than three.
 - C. In no instance should a quantity figure be based upon fewer than three cases.
 - D. In no instance should a quantity figure be released if one case contributes more than 60 percent of the amount.
 - E. In no instance should data on an identifiable case, nor any of the kinds of data listed in preceding items A-D, be derivable through subtraction or other calculation from the combination of tables released.
 - F. Data released by the surveillance program should never permit disclosure when used in combination with other known data.

***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.

This page intentionally left blank