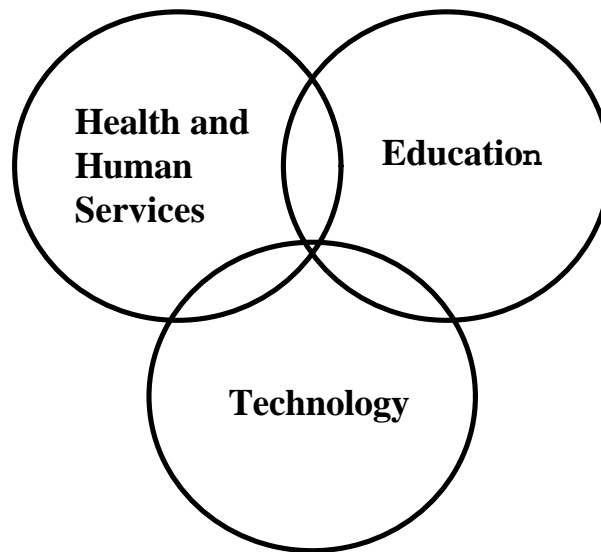


# Model School Health Information System Project



## **SAFEGUARDS AND SECURITY DOCUMENTATION**

January 1996

**Massachusetts Department of Public Health**  
Bureau of Family and Community Health  
Office of Statistics and Evaluation

# MODEL SCHOOL HEALTH INFORMATION SYSTEM

## SAFEGUARDS AND SECURITY DOCUMENT

### Table of Contents

- I. Introduction, Background and Terminology
  - A. Project Purpose
  - B. Terminology
  - C. MSHIS Overview
  
- II. General Guidelines
  - A. Policies and Procedures for School Health Professionals
    - 1. Administrative Issues
    - 2. Recording UHDS Information
    - 3. UHDS Coding Standards
    - 4. Security and Confidentiality
    - 5. End-of-Year Procedures
    - 6. UHDS Changes
    - 7. Permanent Student Identifiers
  
  - B. Policies and Procedures for Information Systems Professionals
    - 1. MSHIS Planning
    - 2. Data Collection and Submission
    - 3. Security and Confidentiality
  
- III. Pilot Demonstration Phase of Project
  - A. Description of Exact Data to be Collected
  - B. Identification of Persons (Organizations) with Access
  - C. Safeguards Employed to Protect Data from Inappropriate Use
  - D. Potential Risks Resulting from Inappropriate Disclosure
  - E. Policies and Procedures Governing Inappropriate Disclosure
  
- IV. Potential Phased-in Statewide Implementation
  - Definitions
  - References

The Model School Health Information System (MSHIS) Safeguards and Security Document includes the following four sections:

- I. Introduction, Background and Terminology
- II. General Guidelines for School Health and Information Systems Professionals
- III. Pilot Demonstration Phase of Project
- IV. Potential Phased-in, Statewide Implementation

Section I provides the background necessary for an understanding of the policies and procedures discussed in the remainder of the document. Since the project involves the cooperation of School Health and Information Systems personnel, Section II is divided into two subsections covering each of these two areas of responsibility. It is important to note that although this document was written specific to the MSHIS Project, many of the policies and procedures apply to any sensitive applications.

During the pilot demonstration phase of the project, there are certain safeguards and security procedures that are being implemented prior to the transmission of data from the local school districts involved in the project to the Massachusetts Department of Public Health (MDPH). In addition, if and when the project continues beyond this initial demonstration phase, further safeguards will be implemented to address issues of ongoing development. Once the data is transmitted to MDPH, it becomes part of the MSHIS Central Repository and is governed by the data management guidelines of the Bureau of Family and Community Health (BFCH). Sections III and IV of this document discuss issues related to the pilot phase and subsequent expansion of the project.

## I. Introduction, Background and Terminology

Providing protection for the rights and welfare of individuals is a matter of serious concern to the general public as well as individuals who design and manage information systems. As McCarthy and Porter (1991) point out, "The rights and welfare of individuals and the rights and welfare of their cognizant communities must be involved in some proportionate balancing of the needs and rights of society to obtain meaningful information relevant to the public health" (p. 238). In addition, they point out that "The publication of the results of a study may have effects on some or all of the members of an identifiable community." They recommend that approval or consent for such studies be obtained from elected or appointed representatives of a community - such as a school board or other community spokespersons. They recommend that studies must be sensitive to the possibility of stigmatizing groups of individuals or communities even when individual data are not released.

## I.A. PROJECT PURPOSE

The purpose of the MSHIS is to develop a national prototype system capable of standardizing data collection across states and reporting health status indicator data from grades K-12. The project purpose, data uses, timelines and general areas covered by the guiding principles and functional specifications have been developed by the Massachusetts Steering, Technical and Region I Advisory Committees associated with the project (refer to MSHIS Final Report issued in April, 1996). MSHIS data will further our current understanding of problems affecting the health, education and welfare of children. When implemented statewide, the data will be used for needs assessment, monitoring state-mandated programs and screenings, program planning and evaluation as well as resource allocation.

## I.B. TERMINOLOGY

- **Authorized Access:** School nurses are the only authorized persons with access to the automated and/or non-automated health information systems. In addition, the nurse may designate other individuals to have access subject to her/his approval. For example, access might be given to the Director of Information Systems for the district if that individual is assisting with the transmission of the data or access may be granted to a substitute nurse.
- **Uniform Health Data Set (UHDS):** The UHDS is a standard developed specifically for the MSHIS project. It defines what student health data is to be collected and how that data is to be coded. It covers a comprehensive set of indicators relating to each student's health status and related data and includes definitions for each data element and the motivation for collecting it. The current release of the UHDS documentation is Version 2.0, dated January 5, 1995. A copy is included in the MSHIS Final Report.
- **UHDS Data Transmission Standard:** The UHDS Data Transmission Standard is a technical document intended to guide information systems professionals in preparing UHDS data for electronic submission to the MSHIS project office. The current version is dated April, 1995 and is included in the MSHIS Final Report.
- **MSHIS Central Repository:** The MSHIS Central Repository is the database that will store the UHDS information for analysis and reporting in accordance with the goals of the MSHIS project. The intent is that it will be located at MDPH. The UHDS standard requires that no student identifying information be submitted to the Central Repository, so all data stored in this database is anonymous. At the Central Repository, all possible steps are taken to ensure that there is no improper access to or use of the data.
- **Joint Committee on the Confidentiality of School Health Records:** As has been recommended by several of the MSHIS pilot demonstration sites, an oversight commission

should be established prior to the reporting of any data to the Central Repository (Confidentiality and Data Security report issued in December of 1994). The report is included in the MSHIS Final Report. The Joint Committee on the Confidentiality of School Health Records addressed the reporting of data during the pilot phase of MSHIS. For ongoing data collection beyond the pilot phase, an oversight commission should be comprised of representatives of all concerned constituencies (parents, students, administrators, public health and information system professionals). This commission should have oversight concerning the uses of the data in the central repository as well as systems development issues.

It was the consensus of the Confidentiality of School Health Records Committee that the highest level of security be implemented regardless of whether aggregate or individual-level data is collected during the MSHIS pilot demonstration phase. Although a decision was made to collect aggregate only data, it is well recognized that data systems evolve over time. As such, the Safeguards and Security Document developed under the MSHIS, was written to reflect appropriate guidelines for the collection and reporting of anonymous, individual level data. This distinction is only relevant at the state level since the data collected at the local level is identifiable and individual by nature. Should the decision be made at some point to collect individual level data, then the more stringent guidelines will already be in place. It is recommended that these guidelines be revisited should the MSHIS become a statewide system at some point in the future.

### I.C. MSHIS OVERVIEW

The collection of UHDS data from the local schools works as follows:

1. Health-related information is recorded throughout the school year by school health professionals (e.g., school nurses) and by school administrative personnel using whatever systems are in place at the local school district.
2. To the greatest extent possible, this information is categorized or coded in accordance with UHDS coding standards.
3. After the end of each school year, the local school or town/city health department/MIS professionals cooperate to collect the UHDS data and submit it to MDPH in accordance with the UHDS Data Transmission Standard. This submission occurs by sending a file electronically or mailing a diskette. Initially, the MSHIS policy was for this file to

include anonymous data for all students leaving grades K, 2, 4, 7, 10 and 12. At the present time, aggregate only data will be shared with MDPH for the aforementioned reporting years.

## II. General Guidelines for School Health and Information Systems Professionals

Because of the wide variety of computerized systems in use at local public schools, it is impossible to provide guidelines specific to each system for recording UHDS information. General guidelines for both school health and information systems professionals are provided here to assist in planning, data collection and administrative issues as well as to minimize potential breaches of confidentiality and security.

### II.A. POLICIES AND PROCEDURES FOR SCHOOL HEALTH PROFESSIONALS

There are a number of system management issues such as back-ups, virus protection, etc. that need to be addressed at the local level. If a network is in place, much of the system management will be handled by the network administrator. If the nurse is using a stand-alone machine, that responsibility rests with her/him.

#### **1. Administrative Issues**

The bulk of the UHDS information submitted under the MSHIS is considered part of the “temporary student record” by the Massachusetts Department of Education (MDOE) student record regulations (603 CMR 23.00: M.G.L. c. 71, 34D, 34F). State and Federal regulations allow access to anonymous information from the student record by state officials (under appropriate circumstances and in accordance with proper guidelines as specified in the MDOE regulations) without the specific informed written consent of the student or parent.

Data transmitted from the local school system to the MDPH is protected under M.G.L. c.111 24A. Data collection under the MSHIS pilot project took place during the last week of January and the first week of February, 1996.

#### **2. Recording UHDS Information**

Each school system has its own system for recording student health information. All pilot site systems involve maintaining this information on a computer, either together with other student records, or as a separate health information system.

The general guidelines for school health professionals are as follows:

- As part of the MSHIS planning process, review each UHDS data element, and determine where that information is most appropriately stored in the automated system. This

planning process should include the information system professional who will be preparing the data for submission, to ensure that the information can be easily extracted and formatted at the end of the year.

- If there are UHDS data elements that do not have an appropriate location in the system, adjust the system if possible to add the necessary capabilities. Again, this may require working with the appropriate information systems professional.
- If it is necessary to collect missing information from parents, make any necessary adjustments to registration or update forms filled out annually by parents in the normal course of school business.
- Technical assistance is available from the MSHIS program in collecting information on computer scannable forms thereby reducing data entry time. Contact the MSHIS program office for further information.
- Technical assistance is available on using hand-held computers or scannable forms for collecting the results of student screenings (e.g. scoliosis, vision, hearing, heights/weights). Contact the MSHIS program office for further information.

### *3. UHDS Coding Standards*

In order to ensure that analysis of the data in the MSHIS Central Repository database is valid, it is important that all school systems follow the same rules in recording health information. The UHDS documents the precise definition of each data item, and the way in which it should be coded when recording information.

For example, the UHDS lists specific codes for recording and categorizing health conditions, assistive devices, medications, and injuries. As another example, heights and weights are recommended to be recorded to the nearest 1/8 inch and 1/2 pound.

In many systems, some health information is entered as freely written text notes. While this is useful as a memory aid during the provision of health services to students, it makes it difficult to standardize data collection. To make submission of standardized data possible, it is important to record the UHDS codes as well as the textual descriptions.

In several cases, the UHDS requests data items that can repeat zero or more times. For example, the UHDS requests a list of all health conditions that apply to the student. If the health conditions are being stored in the computerized health record as a free text field, the UHDS codes should be entered at the beginning of the field, and if more than one applies, the codes should be separated by the vertical bar character (found above the back-slash

character on most keyboards). This applies in situations where a free text field is used to code more than one data item, which may include one or more UHDS elements.

#### ***4. Security and Confidentiality***

UHDS data, as part of the student health record, must be treated with the utmost professional care for privacy of the student and their family. Procedures for securing this information include both physical security and computer security. For more information on security procedures to protect confidentiality refer to Section III.C. of this document.

#### ***5. Backup Procedures***

To protect against loss of data in case of computer hardware or software failure, be sure that regular backup copies of all data are made. In some systems, this happens automatically as part of normal system administration procedures, without any action required on the part of the user. In others, it is the users' responsibility to make backups. Be sure that the security and confidentiality guidelines listed above are followed for all backup storage media (tapes and/or diskettes) as well. Security and confidentiality must be guaranteed if backups are stored off site.

#### ***6. End of Year Procedures***

At the end of each school year, when all data has been entered, the information system professional will extract and format the UHDS data for submission to the MSHIS Central Repository. Depending on the computer systems in place, this may involve the copying of information from the health information system computer to diskette. It is important to stress that once the data is ready for submission, that the nurse review the data to assure that it is accurate to the best of her knowledge.

#### ***7. UHDS Changes***

From time to time, the MSHIS project may make additions, changes or clarifications to the UHDS definition. Notification of such changes will be in written form, and will take effect at the beginning of the next school year.

### ***8. Permanent Student Identifiers***

At the present time, no MSHIS Permanent Student Identifier (PSID) is being used to connect data submitted in one year with data submitted in subsequent years for the same student. Over time, such an identifier would dramatically increase the level of analysis possible using the data in the central repository. If a PSID system is adopted in the future, policies and procedures will be defined covering how identifiers are assigned and how they follow the student across transfers within and between school systems. (See Confidentiality and Data Security Report dated December 1994 in MSHIS Final Report). All school systems involved in the MSHIS project had their own local systems for assigning student IDs. The numbering systems varied with each site.

## **II.B. POLICIES AND PROCEDURES FOR INFORMATION SYSTEMS PROFESSIONALS**

### ***1. MSHIS Planning***

The responsibility of the information systems professional participating in the MSHIS is to prepare the UHDS data in accordance with the UHDS Data Transmission Standard and submit the resulting file to the MSHIS Central Repository after the end of each school year.

Information systems for recording health information and other student records cover a wide variety of system architectures, ranging from fully integrated school management software packages to ad-hoc flat file databases.

At this time, there is no procedure for submitting UHDS information unless the school system keeps information in an automated format. There is no method for submitting this level of information from a non-automated health record that does not involve an inordinate amount of effort on the part of school health personnel.

The general guidelines for information systems professionals are as follows:

- Working with the participating school health professionals, review each UHDS data element, and determine where that information is most appropriately stored in the computer system. The goals should be both to make it easy for data entry and to make it easy to format the data for submission.
- If there are UHDS data elements that do not have an appropriate location in the system, adjust the system if possible to add the necessary capabilities.
- Technical assistance is available from the MSHIS program in collecting information on computer scannable forms and/or hand-held computers. If this is done, the result will be a data file that will need to be loaded into the appropriate locations in the health information system. Contact the MSHIS program office for further information.

## ***2. Data Collection and Submission***

Data should be included only for those students finishing UHDS submission grades K, 2, 4, 7, 10 and 12 as defined in the UHDS. Only students regularly enrolled at the end of the school year should be included, excluding those who transferred to other schools or who are part of special programs that happen to be located in the school building. More detail is provided in the Data Collection, Analysis and Reporting Section of the MSHIS Final Report. Data should be reported only during the year of retention. For example, if a second grade student is retained in the second grade in 1995, data should be reported for that student in 1995. Data should not be reported for that student the following year. Data will be reported on that student again for the year the student finishes the fourth grade.

When notified by the local health professional (school nurse) that all UHDS data entry is complete, this data file must be collected and formatted in accordance with the UHDS Data Transmission Standard. For details on formatting and submission rules, please refer to the UHDS Transmission Standard document dated April 1995 (MSHIS Final Report).

## ***3. Security and Confidentiality***

UHDS data, as part of the student health record, must be treated with the utmost professional care for privacy of the student and their family. The health profession has standards for protecting the confidentiality of records. Information system professionals must treat private data with equally high standards. This includes the following:

- When working with UHDS data, remove information that identifies the individual student as soon as possible in the data preparation process.
- All data disks must be labeled with the following notation: MSHIS: Confidential Data: Unauthorized Use is Prohibited.
- Establish the habit of avoiding looking at sensitive information whenever possible; any private information inadvertently or unavoidably observed must be held in strictest confidence.
- Have all staff involved in the database sign a Security Acknowledgement Form including the holders of the backup copies.

For more information on security measures used to protect confidentiality, refer to Section III.C. of this document.

#### **4. Backup Procedures**

To protect against loss of data in case of computer hardware or software failure, be sure that regular backup copies of all data are made. If this is the responsibility of the end user in your environment, be sure that all users are properly trained and provided with documentation on backup procedures. If backups are part of normal system administration, be sure that the confidentiality guidelines listed above are followed with respect to backup storage media as well.

### **III. Pilot Demonstration Phase of Project**

The MSHIS Uniform Health Data Set (UHDS) collected under the initial pilot demonstration phase does not include an identifier that can be linked back to an individual student. In future phases of the project, the use of a Permanent Student Identifier (PSID) may be tested, however, the PSID can only be matched to the individual student by the local school nurse. The MSHIS was designed so that the MDPH Central Repository could not identify individual students. No individual names or identifiers are included and data will be aggregated in such a way that it is not possible to guess which student profile belongs to which child. See section III.D. for more information.

Prior to data transmission from the local school to the MSHIS Central Repository at the MDPH, documentation should be provided to the local school district submitting MSHIS UHDS data which includes the following:

- Description of exact data to be collected and transmitted to MDPH
- Identification of persons (organizations and other entities) who will have access to the data
- Description of safeguards employed to protect the data from inappropriate use
- Description of potential risks resulting from inappropriate disclosure of the data
- Policies and procedures governing inappropriate disclosure

This document should be sent to the Superintendent of the district as well as to the School Nursing Supervisor.

#### **III.A. DESCRIPTION OF EXACT DATA TO BE COLLECTED:**

The data collected at each pilot demonstration site under the pilot testing phase is not uniform across districts. The collection of data elements at each pilot site, within the UHDS, was dependent upon: (a) the capabilities of the software being used, (b) the degree to which data entry was accomplished, (c) whether or not a supplemental scannable survey was conducted,

(d) the ease with which the data could be collected and (e) the compatibility between the definitions used by the local school district and the MSHIS UHDS. Because the UHDS is an evolving dataset and because neither the MDPH nor MDOE currently have regulations requiring its collection, only those elements collected in the normal course of operations were included. The only exception to this was the use of the scannable form at three of the six sites. Although all of the elements listed below have not been collected at each site, this is an all-inclusive list of the elements that one or more sites are capable of reporting:

- |                                                   |                                            |
|---------------------------------------------------|--------------------------------------------|
| <input type="checkbox"/> Gender                   | <input type="checkbox"/> Days Missed       |
| <input type="checkbox"/> Race/Ethnicity           | <input type="checkbox"/> Sports            |
| <input type="checkbox"/> Date-of-birth            | <input type="checkbox"/> Screening Results |
| <input type="checkbox"/> School Building          | <input type="checkbox"/> Vision            |
| <input type="checkbox"/> Grade                    | <input type="checkbox"/> Hearing           |
| <input type="checkbox"/> Height                   | <input type="checkbox"/> Postural          |
| <input type="checkbox"/> Weight                   | <input type="checkbox"/> Immunization      |
| <input type="checkbox"/> Date of Measurement      | <input type="checkbox"/> Health Insurance  |
| <input type="checkbox"/> Maternal Education Level | <input type="checkbox"/> Physical exams    |
| <input type="checkbox"/> Environmental Smoke      | <input type="checkbox"/> Visits to Nurse   |
| <input type="checkbox"/> Moved Count              | <input type="checkbox"/> Health Conditions |
| <input type="checkbox"/> Emergency Contact        | <input type="checkbox"/> Medication        |
| <input type="checkbox"/> SPED Current             | <input type="checkbox"/> Injuries          |

It should be noted that aggregate only data was reported under the initial pilot testing phase. For more information concerning the data collected from each of the sites, refer to the pilot site-specific reports included in the MSHIS Final Report.

### III.B. IDENTIFICATION OF PERSONS (ORGANIZATIONS AND OTHER ENTITIES) WITH ACCESS:

The following individuals had access to the local confidential school health records themselves during the pilot demonstration phase in order to assure accurate data collection and transmission:

Sabine M. Hedberg, MSHIS Project Director  
Andy Langowitz, MSHIS Technical Consultant

These individuals worked directly with the local school nurses and MIS Director at each pilot site. Signed Security Acknowledgment Forms are on file in the local school nurses office as well as with the Director of the Office of Statistics and Evaluation at MDPH.

Staff from the MDPH Office of Statistics and Evaluation as well as the MDPH School Health Unit will have access once the data is submitted to MDPH through the MSHIS Project Director. Each pilot site was given a copy of their data tables to review prior to submission to MDPH. There should never be identifying information included in the repository housed at MDPH and data should be encrypted. The encryption process is not yet developed. All data analysis and reporting conducted by MDPH will be approved by the Director of the Office of Statistics and Evaluation as well as the Superintendent of the given district, prior to publication. All information requests should be kept on file by the OSE Director.

### III.C. DESCRIPTION OF SAFEGUARDS EMPLOYED TO PROTECT DATA FROM INAPPROPRIATE USE:

The UHDS contains confidential or privileged information about individual students and their families that must be carefully protected against unauthorized disclosure at all stages (This is assuming that individual data may be collected at some point in the future). Although information at the level of individual students may be submitted at some point, the standard for submitting data to the state requires that no identifying information be included once the data leaves the local school system. The anonymous data being submitted must be protected as confidential information by individuals with access. (for more information see section III.D.).

Inappropriate use of the data can occur at four points:

- The local school nurses' office
- Local management information system staff
- Other health professionals at the local school
- MDPH personnel with access to the MSHIS database, file format and encryption used

The local school guidelines listed in section II are intended to protect, to the greatest extent possible, from inappropriate use of data at the first three points. The following steps are being taken at the MDPH to safeguard MSHIS data at the fourth point:

- The Central Repository will be stored on a stand-alone system, not accessible over the MDPH networks.
- The Central Repository computer will be physically located in an office that can be locked.
- Central Repository data will be encrypted using a key that is known only by appropriate MDPH personnel.
- Access to the Central Repository will be controlled through passwords given only to appropriate personnel as determined by the Director of the Office of Statistics and Evaluation and the Director of the School Health Unit

In order to breach this security, a person would have to:

- Gain physical access to the Central Repository computer at the MDPH.
- Decrypt the database or log on to the database with a valid user ID and password.
- Identify individual data, despite the absence of identifying fields.

The above sequence of safeguard violations is highly unlikely to occur. Even though no identifying data is being stored in the Central Repository, there is some risk that anonymous data could be associated with an individual. The primary risk points are the date-of-birth and

the school building codes. The main purpose of the date-of-birth is to allow the computation of nutritional indicators. The following steps could be taken to remove even this low level of risk:

- The date-of-birth and date-of-measurement could be removed from the Central Repository as data is loaded into it, and replaced with a field containing age at measurement.
- Standard MDOE school building and/or school district codes could be replaced by private MSHIS codes, with the correspondence kept in a secure fashion, outside of the Central Repository database.

Given the fact that only test data was collected, a central repository was not established during the initial MSHIS pilot phase. The diskettes with the pilot specific data were submitted to the Director of the Office of Statistics and Evaluation at MDPH. The Director is responsible for the safe-keeping of the data. To reiterate, during the initial pilot testing phase of the MSHIS Project, no identifying individual level data was collected from the local schools participating in the pilot.

Because there can be threats to confidentiality within each step from data collection to analysis, transmission and reporting, guidelines need to be developed at each point. Only staff authorized to utilize or handle the data will be allowed access. All employees must be trained on standard procedures to maintain confidentiality. New employees should be trained in procedures as part of their initial training. Annual refresher sessions should be held for all staff.

All paper records and data diskettes should be stored in a secure place that is protected from unauthorized access. This can be a locked filing cabinet, desk or office. Storage must be secure at all times (school day, weekend, vacations, summertime). In some school districts, staff other than the nurse have access to the health records during the summer when the nursing staff are typically not there. It is the responsibility of the nurse to assure that the databases are secure. Health records transferred from one school to another should be sent from the nurse to the nurse. Health records should not be sent with other school records.

Paper records, diskettes or computer screens should not be left in a state or area where they can be viewed by someone entering the room. It is important to log off from all sensitive computer applications when leaving the computer, even for a short time. All data diskettes should be labeled with the following notation: MSHIS: Confidential Data: Unauthorized Use is Prohibited. The following recommendations should be included in guidelines to be used by all districts participation in the MSHIS.

1. Access to computerized records
  - a. Physical Security: All computers containing MSHIS data should:

- be physically kept in a locked area
  - include a start screen that displays the following message each time the database is entered: "This database is confidential: Unauthorized access is prohibited."
  - include password protection which only allows access to the data by those individuals who have the password. Avoid obvious passwords, change passwords on a regular basis and do not share passwords with others.
  - include a password-protected screen-saver which blocks the screen and only allows the screen to come on if the appropriate password is typed.
- b. All staff with access to computers containing MSHIS data should:
- Have on file with their employer a signed Information Security Acknowledgment Form (ISAF). A copy of the form is included at the end of this report.
  - Understand the requirements of the ISAF and its implications
- c. Staff responsible for backing up the system should ensure security of backup copies of MSHIS files.

2. Protection of paper documentation at the local school

- a. Documents with personal identifiers should be locked in file cabinets when personnel are away from their desk/office.
- b. Staff should not take documents with personal identifiers out of the building unless it is for a field visit. Confidentiality and security must be strictly maintained at these times and documents should be returned to the appropriate files as soon as possible.
- c. Documents with personal identifiers must be shredded prior to disposal.
- d. Printed outputs containing confidential information should be stamped "confidential."

3. U.S. Postal Service by the local school

Guidelines regarding the use of the U.S. Postal Service to transfer data disks and documents that are protected and confidential include the following.

- The name of the specific individual to whom the data is mailed should be clearly marked on the item.
- The item should be labeled as confidential, only to be opened by the authorized person.
- Sturdy envelopes should be used to minimize the risk of accidental tearing.

- If disks are mailed to the MDPH Central Repository, they should be placed in special mailing envelopes designed for disks.

#### 4. Electronic Data Transmission

- a. All data submitted by mail or electronically should be encrypted prior to transmission to MDPH. The technical details of the encryption need to be developed.
- b. Submission by mail or electronic file transfer should be communicated by telephone.
- c. Establish guidelines regarding the security of data transmission via Internet or closed bulletin board systems (only authorized users can log onto the system).
- d. Specific secure procedures need to be in place regarding the sending and receiving of faxes. For confidential data, it is recommended that the sender call the receiver to notify them that a confidential fax has been sent. The receiver can then physically stand at the fax machine at the time the data is being transmitted to limit unauthorized access.

#### 5. Data Reporting

- a. Include a written pledge from MDPH to the local school district that resulting publications of the data will appear only in aggregate form which cannot be linked to individual subjects.
- b. Suppression rules should be employed which do not allow the reporting of any cells less than five to protect confidentiality.

#### 6. Data Retention/Destruction Schedule

Resource and time limitations precluded the development of this component of the Safeguards and Security Document. This section may have important legal ramifications. If the MSHIS files held at the MDPH fall under the public records law, then retention and destruction are governed by the State Records Conservation (SRC) Board. This may mean that all data is to be retained in the state archives.

### III.D. POTENTIAL RISKS RESULTING FROM INAPPROPRIATE DISCLOSURE OF DATA

Inappropriate disclosure of data can occur at both the local school district as well as the MDPH Central Repository, however, these safeguards and security procedures will greatly minimize the risk of inappropriate disclosure. All policies and procedures developed by the

local school and MDPH in regard to automated systems apply with respect to MSHIS data. Raw data will not, under any circumstances, be available to the public.

There are two distinct ways in which individual confidentiality could be violated: first, privacy is violated if someone is able to identify which student corresponds to a given health record, and conversely, privacy is violated if someone is able to retrieve the health record that corresponds to a given student. For more information, see the Confidentiality and Data Security Report dated December 1994. This report provides more detail concerning to potential Permanent Student Identifier (PSID) approach involved in the development of a longitudinal database.

Given the data elements that will be contained within the MSHIS Central Repository, the following breaches of confidentiality are possible should someone gain unauthorized access to the system or should an authorized individual misuse the data:

1. Given the fact that the Central Repository contains the district and building associated with each student as well as their gender, race-ethnicity, date-of-birth, height and weight, it is possible that an authorized person could match a record with a specific individual student. The authorized individual would have the file format of the database and the internal encryption used. Once the data is encrypted, it would be close to impossible for an unauthorized individual to decipher the data.
2. Data could be published on a school-specific or district-specific basis, in the aggregate, without going through the formal approval process at the local school or MDPH.

### III.E. POLICIES AND PROCEDURES GOVERNING INAPPROPRIATE DISCLOSURE:

The following excerpt was taken from the Confidentiality and Security Policy of the MDPH Bureau of Communicable Disease Control dated 7/95.

Employees whose conduct does not conform to the policies set forth in these policies and procedures may be subject to disciplinary action including one or more of the following:

1. Verbal warning
2. Written warning
3. Reassignment of job duties
4. Suspension from job duties
5. Termination

The extent of the disciplinary action will be determined on a case by case basis by the employee's direct supervisor. Employees who willfully or intentionally breach confidentiality with the intent of harming the individual(s) to whom the information is applicable or to the agency will be immediately terminated. Employers may choose to evaluate employees on their performance evaluation based on their ability to maintain confidentiality.

## IV. Potential Phased-in Statewide Implementation

For the 1994/1995 school year, MSHIS data was collected from five of the six pilot site districts throughout Massachusetts: Pioneer Valley School District, Northampton Public Schools/Smith Vocational Agricultural High School, Lexington Public Schools, Minuteman Science and Technology High School and Framingham Public Schools. Data was not reported from the Chelsea Public Schools. Plans are underway to potentially expand to a larger set of pilot sites in 1996/1997 as well as making adjustments to the UHDS based on experience gained from the initial pilot project.

In recognition of the fact that data systems often evolve into something which was not necessarily intended from the onset, and to protect the privacy and confidentiality of students and families, a MSHIS Oversight Committee should be established after the pilot demonstration phase of the project to govern any future developments to assure that the collection and reporting of the UHDS will not adversely affect the rights and welfare of those persons about whom data are collected.

Various analysis and reporting options were considered during the pilot phase of the project which have direct implications for data security. Longitudinal studies provide a greater wealth of information, particularly relevant to the development of prevention programs, however, such studies also require the retention of data linkable over time. Once no further comparisons are planned, identifiers should be destroyed. More detail is provided in the MSHIS Final Report under the section entitled, "Data Collection, Analysis and Reporting." The final report also includes a project overview and section on early project planning, the Region I Advisory Committee, information technology and the Technical Automation Committee, the Permanent Student Identifier (PSID) schema, the Uniform Health Data Set, school health software programs, pilot site-specific documentation, a project evaluation and recommendations for the

future. Copies of the report can be obtained from the Massachusetts Department of Public Health, Office of Statistics and Evaluation.

## MSHIS SAFEGUARDS AND SECURITY PROCEDURES

### Definitions

- Assent:** "A child's affirmative agreement to participate in research. Mere failure to object should not, absent affirmative agreement, be construed as assent" (45 CFR Subtitle A (10-1-91 Edition)).
- Confidentiality:** "How data collected for approved purposes will be protected, maintained and used by the organization that collect it, what further uses will be made of it, and when individuals will be required to consent to such uses" (Protecting Privacy in Computerized Medical Information, 1993).
- Confidential Health Care Information:** "...Information relating to a person's health care history, diagnosis, condition, treatment or evaluation, regardless of whether such information is in the form of paper, preserved on microfilm or stored in computer-retrievable form" (cited in: Protecting Privacy in Computerized Medical Information, 1993: Definition from The American Medical Association's Proposed Revisions to its Model State Bill on Confidentiality of Health Care Information)
- Consent:** An arrangement between parties specifying how information can be shared (discussion at Confidentiality of School Health Records Committee Meeting held August 15, 1995).
- Data Security:** "Protection of data, especially sensitive data, from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration by techniques such as software and hardware protections, physical measures, and informed, alert staff" (Health Data in the Information Age: Use Disclosure and Privacy, 1994).
- Encryption:** "A process of encoding a message so that its meaning is not obvious; decryption transforms an encrypted message back into its normal form. When a message is encrypted, it is encoded in a way that can be reversed only with the appropriate

key. Maintaining confidentiality requires that only authorized parties have the decrypting key" (Protecting Privacy in Computerized Medical Information, 1993).

**Health Care Information:** "...any data or information, whether oral or recorded in any form of medium, that identifies, or can readily be associated with the identity of a patient or other record subject: and 1) relates to a patient's health care; or 2) is obtained in the course of a patient's health care from a health care provider, from the patient, from a member of the patient's family or an individual with whom the patient has a close personal relationship, or from the patient's legal representative" (cited in Protecting Privacy in Computerized Medical Information, 1993): Definition from the American Health Information Management Association's Health Information Model Legislation Language).

**Health Status:** Information typically from individuals themselves, on domains of health such as physical functioning, mental and emotional well-being, cognitive functioning social and role functioning, and perceptions of one's health in the past, now, and for the future and/or compared with that of one's peers (also called health-related quality of life) (HEALTH Data in the Information Age: Use, Disclosure and Privacy, 1994).

**Permission:** "The agreement of parent(s) or guardian(s) to the participation of their child or ward in research" (45 CFR Subtitle A (10-1-91 Edition).

**Privacy:** "The claim of individuals, groups of institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Alan Westin, Privacy and Freedom, 1967 cited in Protecting Privacy in Computerized Medical Information, 1993). \*

**Unique Identifier:** A code (usually numeric or alphanumeric) that refers to one, and only one, person at any one time, does not change for that person over time, and permits positive (or probable) identification of that individual.

**Universal Identifier:** "A single code used in all health databases to refer to an individual. Such a code would allow linkage among health data bases" (Health Data in the Information Age: Use, Disclosure and Privacy, 1994).

---

\* "The balance struck by society between an individual's right to keep information confidential and the societal benefit derived from shared the information" is the issue at hand ("Protecting Privacy in

Computerized Medical Information."

## References

McCarthy, Charles R. and Porter, Joan, P. "Confidentiality: The Protection of Personal Data in Epidemiological and Clinical Research Trials." Law, Medicine and Health Care, Volume 19: 3-4, Fall-Winter 1991, pgs. 238-241.

Draft materials developed by MDPH OSE staff regarding the maintenance of confidentiality of data forms, printed outputs and electronic storage and transmission of data.

Confidentiality and Security Policy of the MDPH Bureau of Communicable Diseases, 7/95.

U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993).

Donaldson, Molla S., and Lohr, Kathleen, N. (Editors) Institute of Medicine, Division of Health Care Services, Health Data in the Information Age: Use, Disclosure and Privacy, (National Academy Press, Washington, DC:, 1994).