MICHIGAN PUBLIC HEALTH INSTITUTE

POLICY AND PROCEDURES

Subject: MPHI Security Policy

Number: 06-02
Revision #3

Date Originally Approved: April 2005
Signature of Executive Director: Jeffrey R. Taylor
Date Revised: December 08, 2009
Signature of Executive Director: Jeffrey R. Taylor

Purpose of Policy:

The purpose of the policy is to ensure: employee safety; protection of MPHI assets; the integrity, availability, completeness, and security of data entrusted to MPHI; the security, integrity, and appropriate use of technical systems; disposal of MPHI-owned equipment in a manner appropriate for a non-profit 501[c][3] corporation; and compliance with the Security Standards set by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Policy Statement:

MPHI provides guidance and procedures enabling staff to maintain the security of health data held in electronic form by MPHI. MPHI promotes a professional and secure workplace while enabling staff to meet federal laws and funding requirements, as well as the needs of clients and the public it serves. MPHI staff, projects, and programs adhere to the Security Standards set by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). MPHI incorporates all HIPAA security requirements into security procedures. MPHI employees maintain a secure environment for the benefit of all personnel. MPHI employees handle MPHI assets, including information systems and telecommunication networks, and disposal of same, in a secure and responsible manner.

Scope:

MPHI is considered a hybrid entity for purposes of HIPAA compliance (see the MPHI Compliance with HIPAA Policy #06-06). As a hybrid entity, MPHI may choose between two courses of action in complying with the Security Rule: (1) The Institute may isolate its covered entity components and apply two security standards, one that is HIPAA compliant for the covered entity components and a lower standard for the rest of the Institute; or (2) MPHI may apply the same HIPAA compliant security standard across the entire Institute. MPHI has chosen to apply the same HIPAA compliant security standard across its entirety for several reasons: (1) MPHI acts as a business associate on multiple projects and is thus subject to many of the requirements of the HIPAA Security Rule on all of those projects; (2) Privacy-sensitive data are not isolated from less sensitive data on the Institute's file servers and other technical systems; and (3) Application of more than one standard to complex, interconnected technical systems is impractical.

All regular MPHI staff, projects, and programs are responsible for complying with this policy and the associated procedures. Full time, part time, and temporary employees are all expected to comply with this policy. Affiliate employees may or may not be required to comply (see guidance contained in the procedure for applying this policy to Affiliated Centers below). It applies equally to information and data processing and communication, whether or not data are owned by or located at MPHI.

Currently, MPHI has two groups that maintain technical systems at the Institute: (1) The Management Information Technology (MIT) group, which is part of the Institute's Central Administration; and (2) The Interactive Solutions Group (ISG), an MPHI program. Each of these groups is required to comply with this policy. Any additional technical groups that may emerge in the future at MPHI are required to comply with this policy.

Purpose of Procedures:

The procedures detail the administrative, physical, and technical safeguards employed to protect the technical systems at MPHI. MPHI technical systems are used to store, access, and/or manipulate health data in electronic form. These systems include the Institute's file servers, email servers, WebDENIS System, DMZ Systems, and SAP. Electronic data stored on removable media are also covered by the policy. Security of hardcopy data is covered in the Confidentiality and Privacy Practices Policy (#06-05).

These procedures keep the technical systems at MPHI as secure as possible and lower the risk of compromise to the data held by the Institute. Employees of MPHI with access to confidential data have the obligation to maintain their accuracy, completeness and confidentiality, whether or not data are owned by or located at MPHI. All procedures guide the activity of MPHI employees working on both standard and privacy-sensitive projects.

Definitions:

Affiliated Center: An MPHI *Affiliated Program or Center* is a group of MPHI Affiliated employees performing project work under the supervision of an MPHI-designated Director or Research Scientist, who may or may not be an MPHI employee. For purposes of this document, Affiliated Programs & Centers will be referred to as *Affiliated Centers*. Affiliated Centers are sometimes housed in facilities outside of MPHI's offices, do not use MPHI's logo or name, and have policy independence as to the content of the work performed. Funding for employee salaries, fringes, and related expenses must come through MPHI. Funding for other project expenses may or may not come through MPHI.

Business associate (BA): This term is more fully defined in each of the HIPAA regulations, but a brief definition is: An organization that works with or for a covered entity in a capacity that involves accessing, using, or disclosing individually identifiable health information. Covered entities must use contracts to require their BAs to also comply with the HIPAA regulations. See the instructions document titled "Is Your Project Privacy Sensitive?"

Covered entity (CE): A covered entity is any of the following: (1) A health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. All covered entities must comply with the HIPAA regulations. See the instructions document titled "Is Your Project Privacy Sensitive?" for more details.

Full Backup: This backup includes all files that are selected and sets the archive bit.

Grandfather-Father-Son (GFS) Method: This is a backup schedule that specifies minimum intervals for rotating and retiring media. Backup is performed at least once a week. All other days, full, partial, or no backups are performed. The daily backups are the Son. The last full backup in the week (the weekly backup) is the Father. The last full backup of the month (the monthly backup) is the Grandfather. By default, you can re-use daily media after six days. Weekly media can be overwritten after five weeks have passed since it was last written to. Monthly media are saved throughout the year.

Health Care Clearinghouse: This a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that performs either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

HIPAA: The Health Insurance Portability and Accountability Act of 1996. The Administrative Simplification subtitle of HIPAA provides the statutory basis for the Department of Health and Human Services to write and enforce various regulations related to electronic data interchange in the US health care system and to the privacy and security of health information.

Hybrid Entity: A single legal entity: (1) that is a covered entity; (2) whose business activities include covered and non-covered functions; and (3) that designates health care components in accordance with paragraph 164.105 of HIPAA.

Incremental Backup: This backup only includes the files that were changed, created, or accessed since the last Full Backup or Incremental Backup. This backup adds to the Full Backup and resets the archive bit after the files have been backed up.

Network Drives: File or data storage located on MPHI servers or other network attached storage, contrasted with "local drives" which are located on individual PCs.

Privacy-sensitive project: A project may be classified as privacy-sensitive due to applicable federal laws such as HIPAA, because of state or local laws or regulations, or by the MPHI Privacy Panel decision. Privacy-sensitive projects are required to comply with additional and/or modified procedures and safeguards that are not normally applied to standard projects (see the MPHI Confidentiality and Privacy Practices Policy #06-05).

Standard project: A project that does not meet the criteria for being a privacy-sensitive project is considered a standard project. Staff on these projects must maintain the accuracy, completeness and confidentiality of all confidential records, reports and data files.

SAP (Systems Applications and Products): This is the MPHI financial information system.

SECURITY STANDARD: SECURITY MANAGEMENT PROCESS

MPHI is required to implement policies and procedures to prevent, detect, contain, and correct security violations.

Procedure: Risk Analysis

The Security Officer (or designee) will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data held by the Institute on a periodic basis. If a 3rd party vendor is chosen to perform this assessment, the vendor will be approved by the Security Officer. More targeted assessments will be conducted on new or problem programs or technical systems as needed.

Procedure: Risk Management

In conjunction with MPHI information technology staff, the Security Officer will implement security measures sufficient to reduce technical system risks and vulnerabilities to a reasonable and appropriate level.

Procedure: Sanction Policy

The HIPAA Privacy and Security Rules require that appropriate sanctions be applied to workforce members who fail to comply with MPHI security policies and procedures. To encourage a culture of compliance, sanctions have been developed that apply at both the individual and program levels. Applying sanctions to individual staff that are non-compliant is most effective at modifying the behavior of those staff and is a necessary component of any sanction policy. Applying sanctions to programs whose staff show a continuing pattern of non-compliance encourages program directors and supervisors to work with problem staff to eliminate issues and encourages individuals within programs to work together as a group to address security issues and incidents. To help apply these sanctions fairly and equally, compliance with the security policy is part of every employee's annual performance evaluation.

[Note: A definition of and examples of security incidents are detailed below in the Security Incident section of this policy.]

Sanctions applied to individual staff involve an escalating series of actions:

1. Repeated security incidents will result in mandatory refresher security training. Employees involved in more than three (3) incidents over the course of one month, or more than six (6) incidents over the course of six months will be subject to mandatory training.

2. After mandatory re-training, the number of violations will return to zero. The violations will still count toward the department total. Employees involved in more than two (2) incidents over the course of one month, or more than four (4) incidents over the course of six months will receive a letter of reprimand in their personnel file.

3. After an employee receives a letter of reprimand, the number of violations will return to zero. The violations will still count toward the department total. Continued violations will result in implementation of a performance improvement plan (PIP). After receipt of a letter of reprimand, employees involved in more than two (2) incidents over the course of one month, or more than three (3) incidents over the course of six months will be placed on a performance improvement plan.

4. Staff who have received a letter of reprimand in the last year and/or been placed on a PIP will be subject to a reduction in the amount of compensation in the form of raises and bonuses for which they are eligible at the time of annual review.

5. Continued violations will result in additional penalties up to and including termination.

6. Flagrant disregard of MPHI security policies and procedures will result in immediate termination.

Sanctions applied at the program level also involve an escalating series of actions:

One month period:

1. The number of violations allowed per department per month is calculated by multiplying the number of staff members by 50%. The Security Officer will calculate these numbers and provide them to the Program Directors no later than the first business day of each month.

2. When 50% of the allowed violations for a one month period have occurred, a meeting will be set up with the Security Officer, Privacy Officer, Security/Telecommunications Specialist, Supervisors, and Program Director to discuss the barriers to employee performance and possible solutions.

3. When 100% of the allowed violations for a one month period have occurred, the entire program will attend retraining. The number of violations will return to zero and the number of allowed violations is recalculated at 75%. (eg. # of staff * 50% * 75% = # of allowed violations).

4. After mandatory retraining, when 50% of the allowed violations for a one month period have occurred, a meeting will be set up with the Security Officer, Privacy Officer, Security/Telecommunications Specialist, Supervisors, and Program Director to discuss the barriers to employee performance and possible solutions.

5. When 100% of the allowed violations for a one month period have occurred, the program will be subject to a 1% reduction in their annual bonus.

Six month period:

1. The number of staff members will be calculated as an average of the number of staff on the first of each month (eg. # staff members * 50% * 6 months / 2 = number of violations per six month period).

2. When 50% of the allowed violations for a six month period have occurred, a meeting will be set up with the Security Officer, Privacy Officer, Security/Telecommunications Specialist, Supervisors, and Program Director to discuss the barriers to employee performance and possible solutions.

3. When 100% of the allowed violations for a six month period have occurred, the entire program will attend retraining. The number of violations will return to zero and the number of allowed violations is recalculated at 75%. (eg. # of staff * 50% * 6 months / 2 * 75% = # of allowed violations).

4. When 50% of the allowed violations for a six month period have occurred, a meeting will be set up with the Security Officer, Privacy Officer, Security/Telecommunications Specialist, Supervisors, and Program Director to discuss the barriers to employee performance and possible solutions.

5. When 100% of the allowed violations for a six month period have occurred, the program will be subject to a 1% reduction in their annual bonus.

6. Programs with 10 or less individuals will be based on a static number of 10 employees.

7. Privacy and security performance of programs will be included in the Program Directors annual review criteria. Program directors whose programs have received mandatory refresher training and a reduction in the annual MPHI bonus will be subject to a reduction in the amount of compensation in the form of raises and bonuses for which they are eligible at the time of annual review.

Procedure: Information System Activity Review

The Security Officer will perform an audit of the assigned access of MPHI personnel to project folders containing privacy sensitive data. The Confidentiality and Privacy Policy (#06-05) requires Project Leaders to maintain a log file of those employees who have been granted access to folders containing privacy sensitive data. The log files are to be submitted to the Security Officer on a quarterly basis for review. The Security Officer will use these forms to update the network permissions as needed. For additional information on the specific requirements of the log file, please see the Confidentiality and Privacy Policy (#06-05).

SECURITY STANDARD: ASSIGNED SECURITY RESPONSIBILITY

MPHI is required to identify the security official who is responsible for the development and implementation of security policies and procedures.

Procedure: Appoint a Security Officer

The Security Rule requires that MPHI appoint one individual with responsibility for the development and implementation of security requirements. MPHI has therefore appointed an MPHI Security Officer.

SECURITY STANDARD: WORKFORCE SECURITY

MPHI is required to implement policies and procedures to ensure that all members of its workforce have appropriate access to data, and to prevent those members who do not have access from obtaining access.

Procedure: Authorization and/or Supervision

All requests for network access must be approved by the appropriate Program Director. This process is facilitated by the Technology Request Form filled out by the staff supervisor and Program Director. MIT provides access to the network and appropriate folders based on these requests.

Procedure: Workforce Clearance Procedure

To ensure that a staff member's access to data is appropriate, MPHI has implemented workforce clearance procedures conducted at the time of hire.

Hiring procedures (for additional information on Hiring Procedures see Policy #02-02):

Once candidates are identified for employment, they are asked to complete an employment application authorizing MPHI to complete a background and reference screening process.

MPHI uses a third party vendor (Justifacts) to conduct background checks on all new employees before they are hired. MPHI verifies educational background as well as criminal (federal, state and county) searches for all employees. Employees employed in positions requiring more than normal access to MPHI's technical systems (i.e., MIT staff) have a more in depth background check completed. This check includes a social security number track as well as the standard criminal and educational checks.

In addition to the background check, MPHI also conducts professional reference checks on employees to ensure that past employment is verified and to review any problems with performance that may have occurred with previous employers.

MPHI cleaning staff are subject to a background check at the time of hire.

Procedure: Termination Procedures

MPHI has implemented procedures to ensure that employee access to data is removed at time of separation:

If the separation is due to termination, a meeting takes place with the Human Resources Manager, the Program Director and/or supervisor, and the employee. The employee is notified that s/he is being terminated, walked to her or his office (or a time is scheduled with the Human Resources Manager after hours) to collect the employee's personal belongings. The employee is escorted out of the building. MIT is notified of the termination by the Human Resources Manager, either before or immediately after the termination takes place. Should an employee need or want personal belongings from her or his computer s/he may contact the Human Resources Manager who will work with MIT staff to retrieve the belongings.

At the time of any separation, MIT removes building security access and locks computer access. MIT disables the employee's network account by changing the password. Voice mail passwords are changed at this point as well. The Supervisor, Program Director or their designee must fill out the Technology Exit Form electronically and submit it to the Telecommunication/Security Specialist within 2 business days of the employee's departure.

Keys, proximity cards, cell phones, palm pilots, etc. are collected at the time of separation. If the employee knows administrative passwords to servers or computers, these passwords are changed immediately.

SECURITY STANDARD: INFORMATION ACCESS MANAGEMENT

MPHI is required to implement policies and procedures for authorizing access to data.

Procedure: Isolating Health Care Clearinghouse Function

If a health care clearinghouse is part of MPHI, the Institute is required to implement policies and procedures that protect the electronic protected health information held by the clearinghouse from unauthorized access by the larger organization. MPHI currently has one healthcare clearinghouse that is maintained by the ISG Affiliate program. The clearinghouse technical systems:

1. Must restrict access to only those employees with authorization to work on the project.

~~2. Must not be connected in any way to the MPHI Network.~~

2. Must require servers be stored in a locked rack.

Procedure: Access Authorization

MPHI must implement policies and procedures for granting access to data. Prior to gaining access to the network and network folders, MPHI staff must follow the procedures below.

1. Supervisors, Program Directors, or their designee must fill out the Technology Request Form and submit it to the MIT department at least 2 business days prior to the employees start date. In the event an employee will be starting in less than 48 hours, the paperwork needs to be submitted immediately following the candidates acceptance of the position. Only after MIT has received these forms will an account be created for the user.

2. Current employees that need additional access must have permission from their Program Director.

Procedure: Access Establishment and Modification

MPHI must implement policies and procedures that, based upon its access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Program Directors of privacy sensitive projects will be required to submit a log file of those employees who have been granted access to project data on a quarterly basis. Please see the Information System Activity Review section above for additional details.

STANDARD: SECURITY AWARENESS AND TRAINING

MPHI is required to implement a security awareness and training program for all members of its workforce.

Procedure: Security Reminders

MPHI will provide periodic security reminders and training in the following ways:

1. All MPHI staff will receive training on the MPHI Security Policy. New employees will be required to complete this training within 2 weeks of their start date. Mandatory retraining for all MPHI employees may be required periodically.

2. The Telecommunication/Security Specialist will provide new hires with training on the proximity card and building alarm systems after their first week of employment. If the new employee needs building access outside of the normal business hours (8am-5pm Monday-Friday) during their first week of employment, special arrangements will be made for their training. The Telecommunications/Security Specialist will conduct refresher trainings with staff as needed.

3. The MPHI Helpdesk will send out security updates and information as necessary.

4. The MPHI Security Officer will send out security updates and information as necessary.

Procedure: Protection from Malicious Software

MPHI is required to implement procedures for guarding against, detecting, and reporting malicious software.

1. Anti-Virus software must be installed on all servers and desktops and updated weekly. Staff with workstations must ensure that the computers remain on, and user logged off, so they can receive their updates during non-working hours. Staff with laptop computers who do not leave them docked overnight, will receive their updates the next time they log into the network.

2. Microsoft critical patches must be installed on a monthly basis. If a system vulnerability is detected prior to the monthly release of patches, the update must be installed immediately.

3. MPHI Staff are not allowed to install any software without prior approval from the MIT department. Please refer to the Software Policy (#04-14) for additional details.

4. Employees are required to fill out the Freeware/Shareware Authorization Form on the intranet and receive MIT approval prior to downloading/installing any Freeware/Shareware applications. Please refer to the Software Policy (#04-14) for additional details.

5. Server/system logs must be reviewed on a bi-weekly basis.

6. If MIT staff or the HEAT Asset Tracker detects spyware/adware on a computer, it must be removed immediately by MIT staff.

7. All MPHI laptops and desktops located off site must be brought into the MIT department no less than on a quarterly basis for updates and HEAT Asset Tracker scanning.

a. All scheduled laptop computers need to be delivered by the respective department(s) to the MIT department by 8:30 AM on their scheduled day(s).

b. Turnover for updating laptops will be less than 24 hours, except for cases where it is impossible to work on the laptop due to unforeseen events or priority work.

c. Scheduling flexibility will be given when possible, but only with the approval of the MIT Director or MIT Support Manager for unusual circumstances or special requests.

d. A mass recall can be used at any time by the MIT department in order to ensure the security and integrity of MPHI owned equipment and data.

e. Any laptop computer that is serving as a user's sole campus workstation does not need to be scheduled for these periodic updates by MIT. If a laptop is being used in conjunction with a desktop computer, the laptop computer will still need to be scheduled for updates by MIT.

7. Web content filtering software will be used to block spyware/adware from entering the network. Web content filtering software also blocks users from downloading items that could be harmful to the system.

8. MPHI maintains several firewalls to block and monitor traffic traveling inbound and outbound from the network.

9. MPHI uses an Intrusion Protection System to block and identify malicious attacks attempting to reach the network.

Procedure: Log-in Monitoring

MPHI is required to implement procedures for monitoring log-in attempts and reporting discrepancies.

1. System logs are monitored for failed log-in attempts.

2. A user's network account will be locked after three failed attempts.

Procedure: Password Management

MPHI employees are required to:

1. Respect the integrity of passwords and/or authentication pass phrases. The exchanging of passwords or seeking the password of others is explicitly prohibited.

2. Change their password every 45 days.

3. Create difficult passwords that must be at least 8 characters long, and contain three out of the following four characteristics: Upper case, lower case, numbers, and symbols.

4. Password changes/resets must be requested by the individual whose account is being changed. If the person is unavailable and there is an extreme emergency, permission to change a password must be given by the employee's Program Director or MPHI's Director of Human Resources.

5. Respect the integrity of passwords used to access MPHI databases through a web portal. The exchanging of such passwords or seeking the password of others is explicitly prohibited.

6. Passwords may not be displayed in open areas such as on sticky notes stuck to monitors or laptops.

7. The sharing of swipe cards and/or alarm codes is explicitly prohibited. In emergency situations, Authorized Security Personnel may provide employees with a temporary code.

STANDARD: SECURITY INCIDENT PROCEDURES

MPHI is required to implement policies and procedures to address security incidents.

Procedure: Response and Reporting

MPHI is required to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to it; and document security incidents and their outcomes. Security incidents at MPHI are actions that compromise the physical and/or technical security of the Institute's systems. They include, but are not limited to, the following examples: Failure to close and lock office doors or windows, failure to arm suite alarms, misuse of alarms, sharing of master, suite and office keys, sharing of proximity cards, sharing of swipe cards and/or alarm codes, storing any items other than the proximity card in the proximity card holders or attaching additional items to the lanyard, leaving space heaters/fans on overnight, sharing of user names and passwords among employees, failure to lock desktops when leaving workstations, and misuse of network and internet privileges in ways that compromise the integrity of MPHI systems. See Security Violations Document on the intranet.

[Note: Security incidents are NOT the same as *Inadvertent Disclosures* of privacy-sensitive data. Inadvertent disclosures are reported directly to the MPHI Privacy Officer and Security Officer. Appropriate handling of inadvertent disclosures is covered in the MPHI Confidentiality and Privacy Practices Policy (#06-05) and the Breach Notification Policy (#06-09).]

Security incidents are reported to the MPHI Security Officer in a number of ways:

1. The Telecommunication/Security Specialist receives reports of security incidents on a daily basis. This information is documented using a Security Incident Spreadsheet and retained to help track program and individual security performance over time. The information is reported to the Security Officer on a daily basis. The Security Officer provides Program Directors with a list of the violations that occurred within their program on a regular basis. Program Directors (or their designee) will address the incidents with individual staff. The Security Officer addresses incidents directly with staff involved in repeated incidents as needed. The Security Officer will also provide the MPHI Executive Officer with a list of security incidents by program on a regular basis.

2. MIT staff reports incidents, such as user name and password sharing, to the Security Officer as they occur. The Security Officer documents the information in the spreadsheet of security incidents mentioned in (1) above. The Security Officer includes this information in the reports she provides to the Program Directors and the MPHI Executive Officer.

3. All MPHI staff are obligated to report any security incidents of which they become aware immediately to the Security Officer. Once reported, the Security Officer documents the incident in the Security Incident Spreadsheet and investigates as needed.

Once reported, Security Incidents are investigated by the Security Officer and Telecommunication/Security Specialist as needed. The Security Officer will always investigate a security incident when the employee(s) involved in an incident disputes its occurrence in any way. The results of the investigation will be reported in writing to the appropriate employees, Program Director and to the Executive Officer.

STANDARD: CONTINGENCY PLAN

MPHI is required to establish policies and procedures for responding to emergencies or other occurrences that damage systems containing health data.

Procedure: Data Backup Plan

MPHI is required to establish and implement procedures to create and maintain retrievable exact copies of health data.

1. MPHI will create and retain backup copies of electronic files for all technical systems within the organization, with the exception of any files stored on local hard drives. These backups protect the data against unexpected loss due to fire, flood, damage to the network servers, and other adverse events.

2. All backup tapes must be encrypted.

3. All backup tapes must be stored at an off-site location.

4. MPHI has a detailed restoration plan in place. For additional information, see the Data Backup and Storage Section of this policy.

Procedure: Disaster Recovery Plan

The Institute has a detailed Disaster Recovery Plan (see policy #04-09) in place. Please see this policy for greater detail. The Security policy deals only with procedures to restore any loss of sensitive and critical data. MPHI data backup and storage procedures make it possible to recover critical data in the event of a disaster/emergency that compromises existing systems.

Procedure: Emergency Mode Operation Plan

MPHI is required to establish procedures to enable continuation of critical business processes for protection of the security of privacy-sensitive information while operating in emergency mode. The Institute has a detailed Disaster Recovery Plan (see policy #04-09) and Emergency Preparedness Plan (see policy #04-04) in place. Please see these policies for greater detail.

Procedure: Testing and Revision Procedure

MPHI must implement procedures for periodic testing and revision of contingency plans. Staff managing each of MPHI's technical systems will perform a data recovery exercise a minimum of once per calendar year. Results must be presented in writing to the Security Officer.

Procedure: Applications and Data Criticality Analysis

MPHI must assess the relative criticality of specific applications and data in support of other contingency plan components. The Security Officer (or designee) will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the privacy-sensitive data held by the Institute on a periodic basis. This risk analysis will include an applications and data criticality analysis. The Security Officer will evaluate the results of this assessment and work with the appropriate staff to mitigate any risks. The contingency plan will be updated accordingly.

STANDARD: EVALUATION

MPHI must perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the HIPAA Security Rule, and subsequently in response to environmental or operational changes affecting the security of health data that establishes the extent to which MPHI security policies and procedures meet the requirements of the Rule.

Procedure: Evaluation

The Security Officer (or designee) will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the health data held by the Institute on a periodic basis. This risk analysis will include an evaluation of environmental or operational changes at the Institute that affect the security of data. The Security Officer will evaluate the results of this assessment and work with the appropriate staff to mitigate any risks. Security policies and procedures will be updated accordingly.

STANDARD: BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS

MPHI may permit a business associate to create, receive, maintain, or transmit health data on its behalf only if the Institute obtains satisfactory assurances that the business associate (BA) will appropriately safeguard the information.

Procedure: Written Contract or Other Arrangement

MPHI is required to document the satisfactory assurances required through a written contract or other arrangement with the business associate that meets the applicable requirements. The MPHI Subcontract Template contains BA terms when appropriate. The MPHI Privacy Officer reviews and approves all BA Agreements into which the Institute enters (see the MPHI Compliance with HIPAA policy #06-06 for additional information).

STANDARD: FACILITY ACCESS CONTROLS

MPHI is required to implement procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed.

Procedure: Contingency Operations

MPHI is required to establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. See the MPHI Disaster Recovery Plan #04-09 and the Emergency Preparedness Plan #04-04 for details on access to facilities under contingency operations.

Procedure: Facility Security Plan

MPHI must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

• Building keys and proximity cards (as applicable) are issued by the MPHI Telecommunication/Security Specialist at the time of each employee's initial orientation, and must be returned at the end of employment.

• Standard hours of operation are from 8 a.m. to 5 p.m. Monday through Friday. All exterior doors are automatically locked from 5 p.m. until 8 a.m. All interior suite doors are to be locked when no employees are present.

• Doors that contain proximity card readers need to remain closed at all times. These doors may be propped momentarily if moving items in or out of the area.

• Employees working outside standard business hours (8 a.m. – 5 p.m., Monday – Friday, and weekends) are responsible for listing their name on the security board located in the foyer of each building. **For their own safety, employees should lock all interior suite doors when working outside of standard hours. (Recommendation. No penalty applied for noncompliance)**

• Closing procedures for all MPHI staff will include:

Shut and lock office windows.

Pull shades.

Shut and lock office doors.

Cross name off the board when exiting after 5:00 P.M. (**Recommendation**. No penalty applied for noncompliance)

• Closing procedures for last person to leave each office suite will include:

Verify that you are the last person in the building by walking through the building and checking carefully.

Ensure all interior and exterior doors are closed and locked.

Ensure coffee pots and other office machinery are turned off.

Ensure lights are turned off. (**Recommendation**. No penalty applied for noncompliance)

Arm the security system.

***NOTE:** Closing procedures differ between buildings/suites. To avoid a security violation, please follow the documentation provided by the Telecommunication/Security Specialist.

Procedure: Access Control and Validation Procedures

MPHI must implement procedures to control and validate a person's access to facilities based on their role or function, including visitors, and to control access to software programs for testing and revision.

1. All proximity card access and keys must be approved by the employee's Supervisor and/or Program Director. This access is also reviewed by the Telecommunication/Security Specialist.

2. All visitors must be escorted in areas where they would have access to health data, such as server rooms. In the event a contractor is hired to perform repair work in these areas, an MPHI employee does not need to remain present for the duration of their stay.

3. Workstations must be locked when not in use. Computers will automatically lock after 10 minutes of inactivity.

4. All employees are responsible for the building keys which they are assigned. Sharing of keys is explicitly prohibited.

5. All MPHI employees are required to sign a Key Authorization & Access Control Form at the time keys and building access are granted.

5. Keys must be removed from the lock after unlocking a door.

6. Employees may not store any items other than their proximity card in their proximity card holder and may not attach any additional items to their lanyard.

7. Employees are required to have their building keys and proximity card with them at all times while at MPHI.

8. Lost, stolen, or misplaced proximity cards, swipe cards, and/or keys must be reported to the Telecommunication/Security Specialist within 24 hours. Any proximity card, swipe card, or key that is later found by the employee who misplaced it, must be returned to the Telecommunication/Security Specialist.

Procedure: Maintenance Records

MPHI is required to implement policies and procedures to document repairs and modifications to the physical components of its facilities that are related to security (for example, hardware, walls, doors, locks). Any changes related to locks, keys, or proximity card readers is handled by the MPHI Telecommunication/Security Specialist. The Director of Human Resources will document and maintain written records of other repairs or modifications needed, the contractor utilized, and the date of the action.

STANDARD: WORKSTATION USE

MPHI is required to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of workstations used to access health data.

Procedure: Workstation Use

MPHI workstations are considered an MPHI telecommunication resource. MPHI telecommunication resources are primarily intended to assist employees in the performance of their assigned tasks. MPHI reserves the right to monitor and log all

network activity, including E-mail, with or without notice, and therefore employees should have no expectation of privacy in the use of these resources.

Use of the MPHI telecommunication infrastructure is a revocable privilege, requiring compliance and conformity with this acceptable use procedure. MPHI programs must enforce this procedure and inform their employees and contractors of this procedure. Contractors, who need and are granted access to the MPHI network, are restricted to only those resources necessary to accomplish their contractual, legal or administratively assigned tasks. Please refer to the Confidentiality and Privacy Practices Policy (#06-05) for additional information and requirements for working at home.

EMPLOYEE RESPONSIBILITIES:

1. Staff are required to make a reasonable effort to inform themselves of and comply with the acceptable use procedures of each system and external network they intend to access, prior to their attempting access.

2. Staff are required to respect the privileges of other employees. Unless authorized to do so, employees shall not intentionally seek information on, obtain copies of, use, modify, or place on openly accessible servers - files and other data which are exempt or excluded from public disclosure pursuant to the U.S. Freedom of Information Act (FOIA), PA 442 of 1976, as amended. Release, distribution and handling of FOIA documents and data must conform to Federal Administrative Procedure 2410.01, issued January 1, 1994 and applicable department procedures regarding denial of FOIA requests and other state and federal laws.

3. Staff are required to respect and comply with the legal protection provided by copyrighted and licensed software to programs and data. Downloading software and other materials is strictly prohibited without first obtaining permission from MIT. No software copy is to be made by any employee without a prior, good faith determination by the MIT department that such copying is, in fact, permissible and that the licensing restrictions have been met. (See the Software Policy #04-14).

4. Staff are required to respect the integrity of passwords and/or authentication pass. The exchanging of passwords or seeking the password of others is explicitly prohibited. Under certain circumstances, it may be necessary for MIT staff to obtain an employee's password in order to troubleshoot issues while an employee is off-site. If this should occur, MIT staff will give the user a temporary password and require the employee to change it once the work is complete.

5. Staff are required to respect the integrity of connected computer systems by insuring that imported binary and executable files are virus free.

6. Staff shall not represent themselves electronically as others. Staff are not to log into a computer and then allow another person to use it.

7. Staff must not circumvent established, system-specific policies defining eligibility for resource access.

8. Staff must be good network citizens by being cognizant of and conservative in the bandwidth demands their applications (especially those using video or image transmissions) make on the network. Employees should use media streaming only for work-related purposes.

9. MPHI employees are required to save project data on the network, not on their desktops/laptops. MPHI employees who take project data off-campus for use outside of business hours or during periods of travel must then save that data back onto the network in a program/department's respective network drive and folders immediately upon return to campus. Privacy-sensitive data may be stored on removable media only if clients require and such storage has been approved by the MPHI IRB/Privacy Panel. Guidelines for privacy-sensitive data storage/usage can be found in the MPHI Confidentiality and Privacy Practices Policy #06-05.

10. MPHI employees are not allowed to disable or change the local administrator password on the desktops/laptops. MIT staff may perform these actions only if they are permitted to do so as part of their job responsibilities.

11. MPHI employees are not permitted to remove the administrative network access from their desktops/laptops.

12. Non-approved devices should at no time be used for convenience or subversion of MPHI network/firewall controls to gain access to the internet/network. This includes, but is not limited to, using the tethered modem capabilities of the Blackberry to circumvent the web filtering content software while on campus.

13. MPHI staff may not connect non-MPHI equipment to MPHI equipment without prior written approval from the MIT Director.

14. All USB thumb drives must be purchased through the MIT department and must be encrypted. Thumb drives that have not been approved by MIT will be confiscated. Certain technology functions cannot be performed using an encrypted thumb drive. If such a situation should arise, a detailed description of the problem must be submitted in writing to the MIT Support Manager. Employees must have written approval prior to using a non-encrypted USB thumb drive.

15. MPHI staff must report any lost/stolen equipment immediately to the Security Officer. This includes, but is not limited to, laptops, USB Thumb Drives and Blackberry devices.

Procedure: Remote Access

This procedure applies to all MPHI employees with an MPHI-owned laptop or workstation used to connect to the MPHI network from off-campus. This applies to remote access connections used to do work on behalf of MPHI, including accessing files, systems and databases, reading or sending email through the MPHI e-mail system client, etc. This procedure does not apply to authorized MPHI web server access, such as MPHI web e-mail and MPHI's web enabled information system; these systems can be accessed from any computer.

1. Staff with MPHI-owned laptops/desktops will have the option to set up VPN access to the MPHI network. Please see the Confidentiality and Privacy Policy (#06-05) for additional requirements.
2. It is the responsibility of employees with remote access privileges to ensure that unauthorized users do not gain access to the MPHI network.
3. Remote access is secure and strictly controlled through the use of passwords, public/private keys with strong pass-phrases, and strong encryption.
4. Remote access is not permitted from non-MPHI equipment.
5. All MPHI laptops must be encrypted using PGP Whole Disk Encryption software.
6. Reconfiguration of a user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. A personal firewall, approved by MIT, must be in use before gaining access to the network remotely.
8. In order to receive access to the network remotely, employees must fill out the Remote Access Authorization Form, which is posted on the Intranet and the official drive.
9. Training on how to access the network will be performed by the MIT Helpdesk or Security Engineer. Additional technical requirements are available from MIT.

STANDARD: WORKSTATION SECURITY

MPHI is required to implement physical safeguards for all workstations that access health data, to restrict access to authorized users.

Procedure: Workstation Security

1. Automatic desktop locking mechanisms determined by MIT are enforced for all employees after 10 minutes of inactivity. Regardless, employees must always lock their computers when leaving their desks.

2. All laptops must be encrypted with PGP Whole Disk Encryption software.

3. Users must log off their computers at the end of each day. The computers need to remain on so they can receive their updates during non-working hours. Employees who do not leave their laptops docked each night will receive their updates the next time they log into the network.

4. Employees must shut and lock their office doors when leaving for the day or for an extended period of time.

STANDARD: DEVICE AND MEDIA CONTROLS

MPHI is required to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain health data.

Procedure: Disposal

MPHI-owned computer and technology equipment, including desktop computers, laptop computers, and other equipment necessary for the accomplishment of project or administrative tasks, shall be inventoried, tracked, and disposed of in an appropriate manner when such equipment is no longer needed or has completed its term of useful service. MPHI-owned office equipment, including fax machines, copiers, and furniture, shall be disposed of in an appropriate manner when such equipment is no longer needed or has completed its term of useful service.

Each MPHI program, center, or administrative program wishing to dispose of unneeded or outmoded equipment shall:

1. Determine that the equipment is no longer needed for its original purpose, or has become outmoded and no longer functions with MPHI systems.

2. Determine the project or other account that originally purchased the equipment, and the purpose of that project/account.

If the equipment is no longer needed for its original purpose, but still functions with MPHI systems, the program shall:

1. Reassign the equipment for use (a) within the unit in MPHI offices or (b) at the home office of a staff member approved to work at home (such arrangements must be approved by the employee's Program Director).

2. Reassign the equipment to another MPHI unit for business purposes. Units to which such equipment may be reassigned include other programs, centers, or administrative groups, and the ILC. [Computers, monitors, and printers shall only be reassigned by the MIT department.] If no MPHI unit will accept the equipment, it shall be disposed of, see below.

If no MPHI unit will accept the equipment, or if the equipment is outmoded and no longer functions with MPHI systems, the equipment will be assessed by the Director of Human Resources [furniture and office machines] or MIT staff [computers, monitors, and printers], and disposed as follows:

1. Furniture and office machines will be stored if they appear useable in the near future, or for as long as the cost of storage does not exceed the cost of comparable replacements. The cost of storage shall be born by the originating MPHI unit if that unit wishes to retain control of the furniture or office machines. If no MPHI unit wishes to retain control of the furniture or office machines, the decision to store/not store shall be made by the Director of Human Resources, with the cost of storage born by the Administrative budget. The Director of Human Resources shall make annual assessments of stored items, with less-useful, older items either made available to MPHI staff or donated to a local charity.

2. MIT staff will pick up any computer equipment that is no longer needed by an MPHI unit and determine how it shall be utilized. Computers may be reassigned for special-purpose use at MPHI that does not require connection with MPHI systems. Computers may be disassembled and useful parts retained. Computer equipment not useful for parts will be donated to a local charity.

3. Before computers are donated to a local charity, MIT staff uses Kill Disk software to perform a low level format on the hard drive making it impossible to retrieve any data that may have been stored on the system.

4. CD-ROMs and DVDs that contain privacy-sensitive information must be destroyed using a CD/DVD shredder.

5. All floppy/zip disks that contain privacy-sensitive information must have the Kill Disk software run on it before throwing it away. Employees may bring their old floppy/zip disks to the Helpdesk for disposal.

Procedure: Media Re-use

MPHI is required to implement procedures for removal of health data from electronic media before the media are made available for re-use.

1. If a computer is being reallocated from one employee to another, it must be completely cleaned off and reinstalled by MIT staff prior to the new employee using the computer.

2. If health data is stored on a CD-RW, the CD must be erased prior to re-using it. If health data is stored on a CD-R the CD cannot be reused and must be destroyed using a CD/DVD shredder.

3. Floppy/Zip disks that contain health data must be formatted prior to being re-used.

Procedure: Accountability

MPHI is required to maintain a record of the movements of hardware and electronic media and any person responsible thereof.

1. All new hardware and software must be purchased through MIT staff. Upon receiving the hardware/software, MIT staff will enter all relevant information into the purchasing database. All computer equipment must be tagged with an MPHI identification tag. All software purchased receives a software identification number. The name of the user for whom the hardware/software was purchased is entered into the database. When the hardware/software is reallocated, MIT staff must update the database with the new information.

2. HEAT Asset Tracker software is used to track the hardware and software movement within the organization.

3. MIT staff is responsible for moving all computer equipment and phones. Employees are not permitted to move any equipment without prior written approval from the MIT Support Manager.

3. Each department that has "general pool" laptops must have a check-out procedure to track the movement of laptops within the organization.

4. All MPHI laptops and off-site desktops must be brought into the MIT department on a quarterly basis for updates and HEAT Asset Tracker scanning.

Procedure: Data Backup and Storage

MIT BACKUP PROCEDURES

MPHI shall conduct routine tape backups so that data can be restored in the event of accidental deletion or catastrophic loss. MPHI will backup all data and databases on the network.

MPHI uses a centralized network backup system to perform daily incremental, and weekly full backups of all information stored on network servers. Tape retention is based on the Grandfather-Father-Son (GFS) method. Each backup can consume multiple tapes. At a minimum, full backups (Father) are performed each week (normally on Friday). Incremental backups are performed Monday – Thursday (Son). The last full weekly backup of a month is retained as the "monthly" backup (Grandfather). MPHI purchases new tapes to replace the media retired the previous year. The MPHI Network Engineer and Network Administrator are responsible for performing or assuring that these duties are performed. Data that is not stored on the network is not regularly backed up by MIT unless specific alternate arrangements are made with the MIT Director. Privacy-sensitive data stored on removable media must be backed up as described in the MPHI Confidentiality and Privacy Practices Policy #06-05.

Holt LAN Backup Procedure

1. Retrieve tape(s) from storage facility courier
2. Load autoloader with appropriate tape(s)
3. Inventory tape(s) so the backup software will recognize them
4. Verify backup jobs are scheduled (Date, Time, Job Name)
5. Remove tapes after job completion
6. Store Monday through Friday and monthly tapes off-site at a tape storage facility.

Okemos LAN Backup Procedure

1. Retrieve tape(s) from the safe or storage facility courier
2. Load autoloader with appropriate tape(s)
3. Inventory tape(s) so the backup software will recognize them
4. Verify backup jobs are scheduled (Date, Time, Job Name)
5. Remove tapes after job completion
6. Store Monday through Thursday tapes in a safe on the Okemos Campus. Friday and monthly tapes are stored at an off-site at a tape storage facility.

Holt and Okemos LAN Jobs

- Monday through Thursday (Daily) – Incremental Backup
- Friday (Weekly) – Full Backup
- Monthly and Year End – Full Backup (Last Friday of the month/Year End)

Holt and Okemos LAN Restore Procedure (User deleted files, corrupt data)

1. Users place a request with the Helpdesk for file restoration
2. Determine needed tape(s) to properly restore data
3. Retrieve tape(s) from off-site storage
4. Load autoloader with appropriate tape(s)
5. Inventory tape(s) so the backup software will recognize them
6. Configure restore job as needed to restore data
7. Verify data integrity with users
8. Remove tapes after job completion
9. Return tapes to off-site storage

Holt and Okemos LAN Disaster Recovery (Backup Server)

1. Restore operating system on backup server
2. Reload the backup software
3. Ensure proper device driver for autoloader
4. Ensure proper device drivers for network
5. Retrieve tape(s) from off-site storage
6. Load autoloader with appropriate tape(s)
7. Inventory tape(s) so the backup software will recognize them
8. Catalog all tapes needed to restore data
9. Restore registry from backup tape(s)
10. Restore ALL data from backup tape(s) (Last full backup and all following incremental backup tapes to date)
11. Verify Data Integrity
12. Remove tapes after job completion
13. Return tapes to off-site storage

Holt and Okemos LAN Disaster Recovery - Servers

1. Restore operating system
2. Ensure proper device drivers for network
3. Retrieve tape(s) from off-site storage
4. Load autoloader with appropriate tape(s)
5. Inventory tape(s) so the backup software will recognize them
6. Catalog all tapes needed to restore data
7. Restore registry from backup tape(s)
8. Restore ALL data from backup tape(s) (Last full backup and all following incremental backup tapes to date)
9. Verify Data Integrity
10. Remove tapes after job completion
11. Return tapes to off-site storage

MPHI uses a centralized backup system to backup the SAP systems. A full backup method is utilized every night along with two transaction log backups that consist of hourly changes to the SAP systems. The tape break down is daily, Monday – Thursday; weekly, Friday week 1-4; and monthly. The first of every year, MPHI purchases new tapes to replace the previous year's tapes. MPHI's Network Engineer is responsible for performing or assuring that these duties are performed.

SAP Backup Procedure

1. Retrieve tape(s) from storage facility courier
2. Load autoloader with appropriate tape(s)
3. Inventory tape(s) so the backup software will recognize them
4. Verify backup jobs are scheduled (Date, Time, Job Name)
5. Remove tapes after job completion
6. Store Monday-Friday and monthly tapes off-site at a tape storage facility

SAP Jobs

- Monday through Sunday – Full Backup

SAP Restore Procedure (corrupt database)

1. Determine needed tape(s) to properly restore data
2. Retrieve tape(s) from off-site storage
3. Load autoloader with appropriate tape(s)
4. Inventory tape(s) so the backup software will recognize them
5. Configure restore job as needed to restore data
6. Verify data integrity with SAP core team members
7. Remove tapes after job completion
8. Return tapes to off-site storage

SAP Disaster Recovery (Backup Server)

1. Load and configure operating system on backup server
2. Apply all necessary hardware driver patches
3. Configure network settings
4. Apply all necessary operating system patches
5. Load and configure database software
6. Apply all necessary database patches
7. Load and configure SAP software
8. Apply SAP kernel patch
9. Reload the backup software
10. Ensure proper device driver for autoloader
11. Ensure proper device drivers for network
12. Retrieve tape(s) from off-site storage
13. Load autoloader with appropriate tape(s)
14. Inventory tape(s) so the backup software will recognize them
15. Catalog all tapes needed to restore data
16. Restore ALL data from backup tape(s) (Last full backup and all Transaction Logs to date)
17. Verify Data Integrity with SAP core team members
18. Remove tapes after job completion
19. Return tapes to off-site storage

SAP Disaster Recovery - Servers

1. Load and configure operating system on backup server
2. Apply all necessary hardware driver patches
3. Configure network settings
4. Apply all necessary operating system patches
5. Load and configure database software
6. Apply all necessary database patches
7. Load and configure SAP software
8. Apply SAP kernel patch
9. Load and configure 3RD party tax software
10. Apply all necessary 3RD party tax software patches
11. Reload the backup software
12. Ensure proper device driver for autoloader
13. Ensure proper device drivers for network
14. Retrieve tape(s) from off-site storage
15. Load autoloader with appropriate tape(s)
16. Inventory tape(s) so the backup software will recognize them
17. Catalog all tapes needed to restore data

18. Restore ALL data from backup tape(s) (Last full backup and all Transaction Logs to date)
19. Verify Data Integrity with SAP core team members
20. Remove tapes after job completion
21. Return tapes to off-site storage

Off-site Storage/Tape Retention

In order to provide disaster recovery capability, backup tapes from the Holt Campus are rotated to a secure off-site storage facility. Each morning, the tapes created during the previous day are cataloged and packaged in a locked container and transferred via courier to offsite storage. Monday through Thursday tapes for the Okemos Campus are kept in a safe on the Okemos Campus. Friday and monthly tapes are stored at an off-site storage facility.

Tape Retention: Daily Tapes are kept for a week before they are over-written, with the exception of the last Friday of the month tape. One Friday (weekly) tape set from each month will be kept for one year, while others will be kept for one month and then over-written. The daily and weekly backup tapes are reused and rotated off-site to a tape storage facility. The monthly tapes are stored off-site at a tape storage facility and never reused.

The backup tapes are maintained in off-site storage according to the following schedule:

- Daily SAP tapes remain off-site for one month
- Daily LAN tapes are stored off-site for 6 days
- Weekly LAN tapes are retained off-site for one month
- Month End LAN tapes are retained off-site for one year
- Calendar Year End LAN tapes remain off-site for six years

Daily and Weekly LAN and SAP tapes are destroyed at the end of each calendar year and new tapes are used. Monthly tapes are destroyed after one year; new tapes are used at the beginning of each calendar year.

Other: Backup jobs are checked daily for time elapsed, byte count (amount of data), and data integrity.

Notification: In the case of a backup failure, the Network Engineer will communicate the failure via e-mail to all employees.

DMZ BACKUP PROCEDURES

ISG uses a centralized network backup system to perform daily incremental and weekly full backups of all information stored on the DMZ servers. Incremental Backups are performed Monday – Thursday, Full Backups are performed on Friday, and on the last Friday of the Month a special Monthly Full Backup is created.

DMZ Backup Procedure

1. Retrieve current day's tape from MIT, and deliver tape from two days previous to MIT
2. Load the tape drive
3. Inventory tape so software will recognize it
4. Remove Tape and store for one business day

DMZ Jobs

- Monday through Thursday (Daily) – Incremental Backup
- Friday (Weekly) – Full Backup
- Monthly – Full Backup (Last Friday of the month)

DMZ Restore Procedure (Accidental Data Loss, User Error)

- Consult user regarding last known instance of good data
- Place request with MIT to retrieve tape from courier from last good date.
- Load tape
- Inventory Tape
- Configure restore job as needed to restore data
- Verify data integrity with users
- Remove tapes after job completion
- Return tapes to MIT to be given to courier

ISG BACKUP PROCEDURES

ISG uses a centralized network backup system to perform daily incremental and weekly full backups of all information stored

on their servers. Incremental Backups are performed Monday – Thursday, Full Backups are performed on Friday, and on the last Friday of the Month a special Monthly Full Backup is created.

ISG Backup Procedure

1. Retrieve current day's tape from MIT, and deliver tape from two days previous to MIT
2. Load the tape drive
3. Inventory tape so software will recognize it
4. Remove Tape and store for one business day

ISG Jobs

- Monday through Thursday (Daily) – Incremental Backup
- Friday (Weekly) – Full Backup
- Monthly – Full Backup (Last Friday of the month)

ISG Restore Procedure (Accidental Data Loss, User Error)

- Consult user regarding last known instance of good data
- Place request with MIT to retrieve tape from courier from last good date.
- Load tape
- Inventory Tape
- Configure restore job as needed to restore data
- Verify data integrity with users
- Remove tapes after job completion
- Return tapes to MIT to be given to courier

STANDARD: ACCESS CONTROLS

MPHI is required to implement technical policies and procedures for electronic information systems that maintain health data to allow access only to those persons or software programs that have been granted access rights as specified.

Procedure: Unique User Identification

MPHI is required to assign a unique name and/or number for identifying and tracking user identity. All MPHI employees are assigned a unique username and password that are required for access to the network. For additional information on password requirements, see Password Management section above.

Procedure: Emergency Access Procedure

MPHI is required to establish and implement procedures for obtaining necessary health data during an emergency. For additional information, see the Disaster Recovery Plan section above.

Procedure: Automatic Logoff

MPHI implements a procedure that terminates an electronic session after a predetermined time of inactivity. Screensavers with automatic locking mechanisms will be enforced for all employees after 10 minutes of inactivity. Employees must always lock their computer when leaving their desk.

Procedure: Encryption and Decryption

All outgoing electronic transmissions of identifiable health data must be encrypted by the sender. MPHI also requires that its partners encrypt data before transmitting it to MPHI. Detailed instructions on how to encrypt an email message can be found on the MPHI intranet. See the MPHI Confidentiality and Privacy Practices Policy #06-05 for a more detailed treatment of data encryption.

STANDARD: AUDIT CONTROLS

MPHI is required to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use health data.

Procedure: Audit Controls

1. Server/system logs must be reviewed on a bi-weekly basis.

2. The Security Officer will perform a quarterly audit of network access to privacy sensitive data. See Information and Security Review Section above.

STANDARD: INTEGRITY

MPHI must implement policies and procedures to protect health data from improper alteration or destruction.

Procedure: Mechanism to Authenticate Electronic Protected Health Information

Where appropriate, MPHI must implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. MPHI user controls protect the integrity of data held by MPHI by limiting access to authorized staff only. Program staff are also responsible for the accuracy of data entry into MPHI systems where appropriate. In such cases, programs are required to integrate data verification processes into their data entry procedures.

STANDARD: PERSON OR ENTITY AUTHENTICATION

MPHI is required to implement procedures to verify that a person or entity seeking access to privacy-sensitive information is the one claimed.

Procedure: Person or Entity Authentication

1. All users must have a unique username and password to gain access to the network.

2. Only authorized individuals have access to the server rooms through the use of a proximity card.

3. MPHI staff shall only place health data in secure data folders on the servers. Secure folders are those to which only authorized personnel have access.

STANDARD: TRANSMISSION SECURITY

MPHI is required to implement technical security measures to guard against unauthorized access to identifiable health data that is being transmitted over an electronic communications network.

Procedure: Integrity Controls

MPHI is required to implement security measures to ensure that electronically transmitted health data is not improperly modified until time of disposal. MPHI user controls protect the integrity of data held by MPHI by limiting access to authorized staff only. Program staff are also responsible for the accuracy of data entry into MPHI systems where appropriate. In such cases, programs are required to integrate data verification processes into their data entry procedures.

Procedure: Encryption

All outgoing electronic transmissions of identifiable health data must be encrypted by the sender. MPHI also requires that its partners encrypt health data before transmitting it to MPHI. Detailed instructions on how to encrypt an email message can be found on the MPHI intranet. See the MPHI Confidentiality and Privacy Practices Policy #06-05 for a more detailed treatment of data encryption.

Procedure: Applying this Policy to Affiliate Centers

Affiliate Center projects are considered under the purview of MPHI policy if they meet the following conditions: (a) the project is conducted by a Center with a Director who is an MPHI employee; or (b) the project is one in which MPHI is the applicant/recipient entity for all project funds.

All other projects in Affiliate Centers are considered under the purview of MPHI unless said purview is contravened by an administrative agreement that defines purview and dictates that the partnering entity holds all responsibility for security practices. MPHI reserves the right to question the appropriateness of the assignment of responsibility. The agreement will confirm that the affiliate has security procedures in place comparable to MPHI procedures for maintaining the security and confidentiality of privacy-sensitive data outlined in this document and in MPHI's Confidentiality and Privacy Practices Policy (#06-05).

When projects are conducted by Affiliate Centers directed by persons who are not MPHI employees, MPHI may have minimal opportunity to: monitor the evolution of project designs, workplans and tasks; enforce compliance with MPHI policies; or have substantial involvement or control over project implementation and work assignments. These projects would be, in effect, unmonitorable by MPHI, and would appropriately be covered by administrative agreements that specify partnering institution responsibility. It is appropriate that the entity with *de facto* control over the project retain responsibility for security practices when the program is not housed on the MPHI campus.

MPHI as a responsible party may conduct its own privacy and security review of any project or may accept the review decision of another entity with which it has an administrative agreement addressing responsibility for privacy and security practices. Because of issues related to monitorability, however, the preferred and expected manner in which MPHI will discharge its obligations in regards to Affiliated Center projects is as follows.

1. Projects will be reviewed by MPHI if the projects are in Centers (1) with Directors who are MPHI employees, or (2) where MPHI is the applicant/recipient entity for all project grant funds.

MPHI reserves the right to also review affiliate projects on a case-by-case basis, and can disapprove a project regardless of the partnering entity's findings. If two reviews are completed and there is disagreement on the findings:

1. Both privacy boards will designate at least one member each to work cooperatively to resolve the issues in preparation for panel resolution,
2. The disapproving panel will consider resolutions to the issues,
3. No use or disclosure of data may be implemented without approval by both panels.

Procedural Documents:

See also Information and Instructions (for Review Process of IRB/Privacy Panel); Compliance with HIPAA policy (06-06); Confidentiality and Privacy Practices Policy (06-05); Security Violations Document and the Employee Handbook. These documents are available on the Intranet or from Quality Assurance staff.

MPHI Policies referenced: #02-02; #04-03; #04-04; #04-09; #04-14; #06-05; #06-06; #06-09.

Noncompliance:

MPHI staff whose conduct does not conform to MPHI's policies and procedures may be subject to disciplinary action as detailed in the Sanction Policy section of this document.

Notes: This policy replaces the following policies: Laptop Security Update Policy #04-11; MPHI Telecommunication Network #04-02; Backup/Recovery of Network Servers #04-08; Equipment Disposal #04-06; and Building Security #04-01

Keywords: Confidentiality, HIPAA, security, privacy, Security Rule, Privacy Rule, Backup, disaster recovery, equipment.