



Policy: Operational Guidelines for the Mississippi Health Information Network

Policy Number: 0901 Original Effective Date: 11-06-2009	Revision Effective Date: 05/02/2012
--	-------------------------------------

A. Background

- A.1. The Mississippi Health Information Network (MS-HIN) is a state entity created to facilitate the electronic exchange of health information between health care entities. MS-HIN provides fast, secure and reliable exchange of health information among health care facilities and clinicians in the state of Mississippi. MS-HIN is not a complete medical history or an electronic medical record. It is a mechanism to facilitate the delivery and exchange of patient health information among health care providers with a clinical need to know. The design and implementation of MS-HIN includes state-of-the-art security precautions to safeguard the privacy of protected health information (PHI).

B. Purpose

- B.1. The purpose of this policy is to:
- B.1.1. Provide information about patients' rights regarding the use and disclosure of their protected health information.
 - B.1.2. Define the access controls and parameters necessary to achieve and maintain an appropriate level of security to protect patient data from unauthorized access and disclosure and to ensure the secure and reliable operation of MS-HIN.

C. Scope

- C.1. This policy is applicable to all users and member organizations of MS-HIN. All users of MS-HIN, senders and receivers of data, have signed and agreed to the MS-HIN Participation Agreement and Business Associate Agreement. This policy does not supersede or replace any Health Insurance Portability and Accountability Act (HIPAA) privacy and security policies in use by or applicable to individual MS-HIN users and member organizations.
- C.2. This policy applies to the delivery and query of information through MS-HIN for the purposes of clinical treatment, payment or administrative actions.

D. Definitions

- D.1. *Access Controls* – system level security that grants authorization to view protected health information in MS-HIN.
- D.2. *Auditing* – the logging and monitoring of all system activity, including without limitation: user log-in identification, user name, user organization, date and time, patient account that was accessed, and type of records viewed by user.
- D.3. *Data Contributing Organizations* – those health care facilities that meet the requirements for participation in MS-HIN and are authorized to send clinical data (e.g. lab results) to health care providers/clinicians through MS-HIN.
- D.4. *Expanded Query Access* – allows a user to temporarily extend his or her access rights under defined parameters to view clinical information available through MS-HIN for a Permitted Purpose on a need to know basis.
- D.5. *Health Care Providers/Clinicians* – health professionals licensed in Mississippi with the authority to order or prescribe clinical tests and diagnostics, including without limitation those designated as MD, DO, PA, and NP.
- D.6. *HIPAA* – the Health Insurance Portability and Accountability Act (HIPAA) and all regulations issued pursuant to such statute as both are amended from time to time, enacted to help protect the privacy and security of an individual's protected health information and to require adoption of national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.
- D.7. *Individually Identifiable Health Information* – a subset of health information as defined in HIPAA, including without limitation demographic data and past, present, or future health condition information collected from an individual that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and that is created or received by a health care provider participating in MS-HIN.
- D.8. *Member Organizations* – those who are sending data into MS-HIN as well as those who benefit from the system, such as health plans and employers. Member Organizations have a responsibility to MS-HIN both financially as well as to ensure accurate delivery of data into the system for consumption by MS-HIN users for the delivery of clinical care.
- D.9. *Misuse* – misuse by a MS-HIN user includes without limitation accessing or viewing information on a relative or acquaintance with whom no clinical relationship or need to know exists (e.g. parent, spouse, sibling, child (even under 18 years of age), significant other, co-worker, neighbor) or using MS-HIN for a purpose that is not a Permitted Purpose.
- D.10. *Need to Know* – means that, in order to safeguard patient privacy, MS-HIN users shall receive access only to the minimum functions and privileges required for performing their jobs. The minimum necessary standard does not apply to disclosures to or requests by health care providers for treatment purposes.
- D.11. *Participant* – those health care providers which includes Data Contributing Organizations, Users and data requestors who meet MS-HIN participation requirements and have signed the MS-HIN Participation Agreement.

- D.12. *Permitted Purpose* – A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities. A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.
- D.13. *Protected Health Information or PHI* – means Individually Identifiable Health Information (IIHI) that is protected under HIPAA as defined at 45 C.F.R. section 160.103.
- D.14. *Query* – allows an authorized user who has an established relationship with a patient to search for clinical information for that patient available through MS-HIN on a need to know basis and only for a Permitted Purpose.
- D.15. *Users* – those who enroll in MS-HIN and have been authorized to receive clinical results and reports. MS-HIN users are clinicians and their designated staffs, who must agree to maintain the privacy and security of the information they obtain from MS-HIN. MS-HIN users receive clinical results and, when available, may also query MS-HIN for clinical history.
- D.16. *User Authentication* – MS-HIN requirements for users to gain authorized access to the MS-HIN application.
- D.17. *User Roles* – rules defined by MS-HIN and assigned to users, determining an individual’s level of access to PHI through MS-HIN.

E. Patient Privacy

E.1. Notice to Patients Regarding MS-HIN

- E.1.1. Patient privacy is of critical importance. MS-HIN complies with state and federal laws, including HIPAA. With the assistance of privacy officers from participating hospitals and health systems, health care providers, legal counsel and the MS-HIN Privacy and Security Committee, MS-HIN established a policy that considers the patients’ rights and expectations while balancing the need for health care providers to have information that enables them to make informed decisions and ultimately to provide better quality health care services.
- E.1.2. MS-HIN users shall implement appropriate procedures to (1) inform patients that they use MS-HIN, and (2) inform patients of certain functions in MS-HIN.
- E.1.3. MS-HIN shall make available to users a toolkit to assist in responding to patient inquiries about MS-HIN. This toolkit includes: patient information sheet, MS-HIN Talking Points, privacy and security overview, Non-Participation Request Form, and Reinstatement of Participation Form.

E.2. **Uses and Disclosures of Individually Identifiable Health Information**

- E.2.1. Disclosure of Individually Identifiable Health Information. MS-HIN PHI is not sold or disclosed for any activity that may support marketing (as defined under HIPAA) to the individual nor is individual information provided and/or used for mailing lists.
- E.2.2. Query Access. Only users enrolled in MS-HIN who have an established clinical relationship with a patient will have access to that patient's information available through a query in MS-HIN. Emergency care personnel will have full access to MS-HIN whereby they can access patient records for treatment purposes in emergency care situations.
- E.2.3. Expanded Query Access. Users may expand their access to PHI by requesting to establish a relationship with a patient in MS-HIN. Users are required to log a reason for the relationship. Refer to the Expanded Query Access (Section F.6) for specific details related to this function.
- E.2.4. Audit Reporting. Patients are provided the means and opportunity to request an audit report that identifies which MS-HIN user(s) has accessed their PHI through MS-HIN. Audit reports will not contain any PHI. Specific procedures established, instruct patients how to request audit reports.
- E.2.5. Compliance with Law. All disclosures of PHI through MS-HIN and the use of such information obtained from users of MS-HIN shall be consistent with all applicable federal and state laws and regulations and shall not be used for any unlawful discriminatory purpose. Users that misuse and violate the privacy of PHI are subject to immediate suspension and/or termination of access to MS-HIN up to and including legal action in accordance with MS-HIN's privacy policy and with all applicable federal and state laws and regulations.

E.3. **Patient Non-Participation**

- E.3.1. Patients may decide not to participate in MS-HIN, whereby their PHI will not be accessible by users (including emergency personnel) through a query or expanded query. Patients will be required to complete Non-Participation Request Forms.
- E.3.2. Patients do not have an option whether to participate in delivery of results through MS-HIN. This function is a business-to-business process established between a participating health care provider that orders a test/procedure and the facility that performs the diagnostics and delivers the results.
- E.3.3. Patients who previously chose not to participate in MS-HIN may choose to participate in the system again at any time with no penalty. Patients will be required to complete a Reinstatement of Participation Form.
- E.3.4. MS-HIN developed specific procedures to process both non-participation requests and requests to begin participating again.

E.3.5. Member organizations and users must adopt procedures for notifying MS-HIN of requests from patients not to participate. MS-HIN shall respond to these requests according to the operating procedures that are established.

E.4. Amendment of Data

E.4.1. In accordance with HIPAA, patients are provided the means to challenge and amend their PHI. Requests to amend data shall be made to the data contributing organizations; MS-HIN does not have the authority or access to amend PHI.

F. Information Security

F.1. Access Controls

F.1.1. Only authorized users are granted access to MS-HIN, and users are limited to specifically defined, documented and approved levels of access rights.

F.1.2. Access control to MS-HIN is achieved via identifiers that are unique to each user and provide individual accountability and enable tracking.

F.1.3. Access rights are based on user roles and job responsibilities. The Member Organization and health care provider enrolled in MS-HIN are responsible for creating staff accounts and assigning user roles to those who work for them. Users must be granted access to information on a need to know basis. That is, users must receive access only to the minimum functions and privileges required for performing their jobs.

F.1.4. Users will be required to acknowledge and accept the Terms and Conditions of Use statement prior to logging into the MS-HIN application.

F.1.5. Users will be held responsible for all actions conducted under their sign-on.

F.1.6. Any user accessing the MS-HIN application must be authenticated. The level of authentication will correspond appropriately to the designated access rights.

F.1.7. When a user is inactive for a period of time, as defined by MS-HIN and consistent with HIPAA, the application will automatically time-out. Users will then be required to log-on again to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

F.2. User Authentication

F.2.1. To obtain access to the MS-HIN application, an authorized user must enter his/her unique user identification and supply an individual user password.

F.2.2. To obtain a new password from MS-HIN, users must be able to provide the answers to unique questions selected and answered by the user at the time of set-up.

- F.2.3. All users will be required and prompted to change their passwords at a time interval defined by MS-HIN and consistent with HIPAA.
- F.2.4. Passwords must be promptly changed if suspected of being disclosed to unauthorized parties.
- F.2.5. At the time a user is no longer associated with or employed by a member organization, the member organization is required to terminate the user's access to MS-HIN.

F.3. **User Roles**

- F.3.1. MS-HIN will define, document and maintain user roles created in the application and establish a process for periodic review.

F.4. **Access Rights**

- F.4.1. Users' access will default only to their organization's data. Only pre-defined and approved users will be allowed to obtain expanded access to PHI through MS-HIN.
- F.4.2. Expanded Query Access is an access level that enables a user to temporarily expand his or her standard security rights to view PHI available through MS-HIN on a need to know basis. Refer to Section F.6 "Expanded Query Access" for information specific to this function.

F.5. **Audit Controls**

- F.5.1. MS-HIN logs and monitors all system activity, including: user log-in identification, user name, user organization, date and time, patient account that was accessed, and type of records viewed by a user. Audit reports do not contain PHI.
- F.5.2. MS-HIN shall audit access to individually identifiable health information on a regular and scheduled basis to ensure appropriate use of the system. Auditing procedures define this process.
- F.5.3. Patients are provided the means and opportunity to request an audit report of who has accessed their health information through MS-HIN. Specific procedures established by MS-HIN define protocol to respond to patients' requests for audit reports.

F.6. **Expanded Query Access**

F.6.1. User Requirements

- F6.1.1. The capability of a user to obtain expanded query access is established by the MS-HIN user roles.
- F6.1.2. If expanded query is utilized, the user must indicate a reason, from a pre-defined list of options, as to why he or she has expanded his or her access rights.

F6.1.3. Each time expanded query is utilized, the user must also indicate the period of time for which he or she needs to have access to the patient's PHI, ranging from one single time to a period of time not to exceed six (6) months.

F.6.2. Auditing

F6.2.1. MS-HIN logs and monitors all expanded query access activity, including without limitation: user log-in identification, user name, user organization, date and time, patient account that was accessed, the reason the user utilized expanded query, time period for which access was established, and the type of records viewed by user.

F6.2.2. Patients are provided the means and opportunity to request an audit report of who has accessed their health information through MS-HIN, including utilization of expanded query. Audit reports do not contain personal health information. MS-HIN shall establish specific procedures to respond to patient requests for audit reports.