

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: General Policy Regarding HIPAA Regulations

Policy No: 1

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

Overview- The Arkansas Municipal League (AML or League), Municipal Health Benefit Fund (MHBF or Fund) is subject to three components of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These three components relate to Privacy, Security and the Electronic Data Interchange (EDI) of Protected Health Information (PHI). PHI is generally defined as any individually identifiable health information that is transmitted or maintained in any form that could identify or could reasonably be used to identify the subject of the information. This would include all forms of information, including but not limited to, paper records, electronic records or oral communications. PHI data elements include any of the following: name; address; birth date or age; telephone number; medical record number; biometric identifiers; health plan numbers; occupation; photos; or employer.

EDI- On April 18, 2002, the AML/MHBF made it's filing electronically and received an extension to October 2003 in which to implement the EDI provisions of the regulation. Working with USSI, the AML/MHBF installed the X12 interface program, which gives the Fund's current operating system the ability to receive and transmit information in the proper EDI format. The data to be electronically received and transmitted, as originally prescribed by HIPAA, are the following transactions: claims; eligibility; referral certification and authorization; health claim status; enrollment and disenrollment; claim payment and remittance advice; premium payments; and coordination of benefits. The HIPPA security regulations have added two additional transactions: health claim attachments; and first report of injury. The Fund has installed the appropriate X-12 computer software in order to receive electronic claims etc., but to date no provider has sent claims to the program electronically.

PRIVACY- New Privacy rules became effective April 14, 2003. In order to comply, the MHBF, AML, and Fund management have reviewed and documented the Fund's current and expected future data flows, in order to ensure the awareness of all PHI information exchange points, files and records. Fund management has assessed the Fund's current procedures and made additions and enhancements where needed. Management's direction to BMI (AML/MHBF's third part administrator until July, 2002) to cease the practice of mailing "city reports", which contained PHI, to member municipalities and the elimination of access for some "non-health benefit employees" to the AML/MHBF computer system are examples of proactive changes taken by AML/MHBF management. Management has also prepared and published numerous Privacy Policies and Procedures (see the following). These policies and procedures

have been incorporated into the training programs given to Fund or other appropriate employees, initially and periodically, as may be needed to ensure compliance with HIPAA.

Security- This component of the HIPAA regulations establishes rules requiring that health plans, in this instance the AML/MHBF, have security standards in place to comply with the statutory requirements of HIPAA, and in particular, that identifiable PHI be protected to ensure privacy and confidentiality electronically transmitted or stored. AML/MHBF management has reviewed and documented current, and future, security measures and needs. Specifically, the AML/MHBF has reviewed physical, personnel, paper and electronic security issues and will continue to make adjustments and additions as needed. The addition of a "Firewall" to the AML/MHBF computer system is a prime example of a major security enhancement. AML/MHBF has also documented certain security matters in Policy and Procedure form. AML/MHBF has reviewed the new security rule (effective April 22, 2005) and will make any necessary physical or administrative adjustments to that effective date.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Privacy and Security Officer

Policy No: 2

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

Regulations require that the AML/MHBF designate a PRIVACY OFFICER, who is responsible for the development and implementation of policies and procedures necessary to successfully comply with HIPAA. In addition, due to the anticipated increase in EDI of PHI, as well as new physical and information technology security issues arising out of the new security rule (effective April 2005), the AML/MHBF has also chosen a SECURITY OFFICER. Currently the AML/MHBF has combined these two responsibilities into one position as allowed by regulation with the following responsibilities:

- POLICIES AND PROCEDURES – identification, implementation and maintenance of both privacy and security related policies and procedures.
- RISK ASSESSMENTS – initial and periodic assessments and adjustments of work flows, data flows and physical access to both manual and computerized data.
- FORMS; NOTICES; AND MATERIALS – maintain appropriate privacy and confidentiality consent, authorization forms, information notices and material reflecting the AML/MHBF’s legal practices and requirements.
- TRAINING – delivery of initial privacy and security training to employees, volunteers, medical and professional staff, contractors, business associates and appropriate third party organization employees.
- MONITOR OUTSIDERS – compliance monitoring of all trading partners and business associates to ensure all privacy concerns, requirements and responsibilities are identified and appropriately addressed.
- TRACKING AND REPORTING – establish a mechanism to track access to PHI (within the purview of AML/MHBF) and to allow only authorized and qualified individuals to review or receive reports of such activity.
- INFORMATION ACCESS – ensure member rights to inspect and amend records, as well as to restrict access to PHI where appropriate.

- COMPLAINT PROCESS – establish and administer a process for receiving documenting, tracking, investigating and taking action on all complaints concerning compliance with HIPAA or other related laws or regulations.
- APPLICATION OF SANCTIONS – working with AML/MHBF staff and departments to ensure compliance with privacy practices, as well as consistent application of sanctions for failure to comply with these policies, not only with regard to the AML/MHBF workforce, but also to any extended or related workforce or business associate.
- AWARENESS – promote activities to foster information privacy and security awareness within AML/MHBF and its related entities.
- SYSTEM RELATED SECURITY – review all security plans to ensure alignment between security and privacy practices between departments (i.e.: firewalls; HIPAA system upgrades; information hand-offs; need to know rules; disaster planning/recovery)
- INFORMATION RELEASES – work with all relevant AML/MHBF personnel to ensure understanding and compliance with the policies and procedures.
- STAY CURRENT – maintain current knowledge of laws, accreditation standards and monitor advancements in information technology.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Privacy – General Issues

Policy No: 3

Dates: Original 12/11/02 Latest Revision _____

Executive Approval _____

HIPPA regulations have, for the first time ever, instituted a national standard for the use and disclosure of certain health related information. These regulations establish individual rights regarding PHI. They set forth administrative procedures to ensure the confidentiality and appropriate use of PHI, and became effective for covered entities, such as the AML/MHBF, on April 14, 2003.

As a general rule, a covered entity may not use or disclose PHI except as required, or permitted by the rule, and then only the minimum necessary information needed to carry out the reason for the use or disclosure.

Covered entities include primarily Health Plans (AML/MHBF), Health Care Clearing Houses (public or private entities that convert PHI from nonstandard formats into HIPAA standard formats, or vice versa), and Health Care Providers.

Covered entities may share PHI with entities that use or disclose the information to perform member or health operation functions for or on behalf of the Covered Entity (i.e.: claims processing, utilization review and practice management, legal, actuarial, accounting, consulting, accreditation, data aggregation, and financial services), so long as these “Business Associates” are contractually bound to appropriately safeguard the information and the covered entity properly addresses situations where its business associates fail to comply with primary obligations (see policy # 9 Dealing with business associates).

Covered entities should have contracts with Business Associates that bind them to the safeguarding of information. This is known as a Business Associate Agreement (BAA), and the MHBF is complying with this requirement.

PHI is individually identifiable health information that is transmitted or maintained in any form, which identifies or could reasonably be used to identify the subject of the information. PHI encompasses information in any form including paper, electronic or oral communications. For levels of disclosures and authorizations/consents needed see policy #10.

HIPAA further requires that covered entities adhere to a MINIMUM NECESSARY DISCLOSURE standard for the using, disclosing or requesting of PHI necessary in order to accomplish the purpose requiring the disclosure.

As a practical application of the concepts of HIPAA, AML/MHBF has identified employees and vendors who need access to certain categories of PHI in order to carry out their assigned duties, trained these people, initially and with periodic updates, (See policy #5 Training) and limited access to information (computer passwords, physical records, etc.) to the maximum extent possible while still allowing for the productive and timely processing of claims. AML/MHBF has also established procedures regarding individual requests for PHI (See policy #7 Rights to Protect Health Information).

In summary, AML/MHBF has implemented and will regularly reassess its administrative, technical, and physical safeguards to protect PHI from disclosure or use in violation of HIPAA privacy rules.

AML has also put into place (See policy #8 Complaint Process) a process for dealing with complaints alleging misuse or illegal disclosure of PHI and a process (See policy #6 Employee Sanctions) to deal with employees who cause or aid in such misuse.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Security

Policy No. 4

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

COVERED ENTITIES such as the AML/MHBF must assure customers (patients, healthcare providers etc.) that the confidentiality and privacy of health care information electronically collected, maintained, used, or transmitted is secure. Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission.

The purpose of security is to protect both the system and the information moving through it from unauthorized access and misuse from within.

Risks to security can be passive in nature such as fires, floods, power outages or equipment outages. Risks can also be active hackers, viruses, or disgruntled persons. These later risks must be actively managed.

Experience suggests that security in the electronic environment is derived from both technical safeguards as well as behavioral safeguards. Experience further suggests that only twenty percent (20%) of security comes from technical safeguards, such as hardware or software. While these technical controls must be in place in order to provide maximum security, the AML/MHBF believes that eighty percent (80%) of security issues relate to behavioral safeguards, such as policies and procedures.

In specific terms, Security has been divided in three components by the “Final Security Rule” dated February 20, 2003: SAFEGUARDS; ADMINISTRATIVE PROCEDURES; and PHYSICAL SAFEGUARDS and TECHNICAL SAFEGUARD.

A. Administrative Safeguards

- A security management process encompassing Risk Analysis and management, an information System Activity Review and a Sanction Policy to deal with violators/violations.
- Specifically assign security responsibility to an officer of the organization.

- Workforce security procedures including authorizations and clearance compatible with job duties and procedures to insure terminated employees do not have continued access to systems or files.
- Security awareness and training including security reminders, protection from malicious software and password management.
- Response and reporting procedures for security incidents.
- Contingency plans including data back up plans, disaster recovery plans and emergency made operating plans.
- Business Associate Contracts

B. Physical Safeguards

- Facility access controls including a facility security plan.
- Workstation use and security, including passwords, screen savers etc.
- Device and media controls including disposal of hardware, data backups and storage.

C. Technical Safeguards

- Access controls including unique user identification, emergency access procedures and automatic logoff.
- Person or entity authentication.
- Transmission security including the encryption and decryption of sensitive data.

Within the three general components of safety there are 20 REQUIRED specifications (12 Administrative; 4 Physical; 4 Technical) that must be met and 22 others that must be addressed and finely documented.

With these issues in mind, the AML/MHBF has to date taken a multi-faceted approach to securing electronic data by addressing, in general, the following issues:

Data Integrity – Program software and files have been password secured, and password access has been limited to a “must have to accomplish your job” level. Programmers and those who have password access to data are screened, trained and monitored to ensure no data is inappropriately changed.

Encryption – Data received or transmitted via the Internet (including Health Care Clearing Houses, individual health care providers, etc.) will be properly encrypted to ensure no unlawful access.

Entity Authentication – The AML/MHBF provides mechanisms for authenticating the entry with which communication is being attempted.

Firewall – A comprehensive Firewall has been installed, covering internal computer systems. Thus, the AML/MHBF will be able to constantly monitor and control any entity given the ability to communicate with our systems through this device.

Media Controls – Ensure that proper control over personal computers and other entry equipment is maintained. Control of personal computer screensaver applications and the introduction of any new software to the system or individual personal computers.

Role Based Access Controls – Closely monitor who has access to specific information. For example, MHBF management, billing clerks, claim processors, etc., all have different levels of need regarding PHI. Every attempt possible will be made to ensure that each employee has only the access authorization needed to accomplish his/her assigned job.

Data Back Up Plans – AML has created and is maintaining a Disaster Recovery Plan (DRP). This DRP will grow and strengthen with time and experience as the AML/MHBF familiarizes itself with potential critical events and specific needs. The AML/MHBF will have not only back up information but also access to an alternative “hot site”, through a contract with Sungard Disaster Services, Inc.

Between the date of this policy revision and April 22, 2005, the AML/MHBF “HIPAA Working Group” will review and finalize changes needed in order to comply with the “Final Security Rule”.

Detection, Reporting, Containment and Correction of Security Violations

All employees of the AML are encouraged to be alert for and recognize real or potential security issues. Employees of the IT Department and the MHBF have an even greater responsibility for detecting such issues.

If security issues are detected, the detecting employee should immediately notify the AML Privacy/Security Officer (PSO). If not immediately available, notify the primary IT technology lead employee. Notification can be verbal or email but should be done ASAP.

The Privacy/Security Officer will keep records of notifications, record investigation and actions taken. PSO will also determine if the security issue has allowed a privacy violation and take appropriate action to deal with such.

PSO will keep the AML Executive Director, the IT Technical Lead, the MHBF Assistant Director and the MHBF Board abreast of issues, findings and actions taken.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Training

Policy No. 5

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

Initial training and supplemental training of staff members is a very important component of the AML/MHBF HIPAA compliance strategy. Training covers data privacy and security rules, data vulnerability, and safe data practices which all ensure the protection of PHI in the possession of the AML/MHBF.

A HIPAA training and explanation module has been incorporated within the AML employee handbook. New employees must read and attest in writing that they understand the content of the handbook.

Before the legal effective date of the HIPAA compliance rules (April 2003), an “all hands” session was conducted, explaining in general what HIPAA requires, why it’s required, and the penalties to both the AML/MHBF and individual employees who knowingly or carelessly violate such rules. This basic awareness training was delivered to all staff members, including management and Fund board members. These topics will be revisited, at the very minimum annually, and will receive continual emphasis with the use of unscheduled periodic reminders.

Prior to the legal effective date of the HIPAA privacy rules, as discussed above, all persons directly engaged in the “Health Plan” process received extensive formal training. This training explained the HIPAA requirements, including AML/MHBF approaches, policies, and procedures, and the definitions of PHI, levels of consent, security, etc. including all general information that “hands on” workers need to know and understand in order to properly secure or disseminate PHI as each specific situation requires. Issues related to virus checks, password management and logon/ logoff procedures were also emphasized. Trainees will be given frequent reminders related to HIPAA regulations and other related matters, as well as periodic refresher training. New staff members hired into the AML/MBHF will be given training as is practicable. Changes, additions or eliminations to HIPAA regulations will be communicated to employees as soon as they are known to management.

The AML/MHBF Fund Management and the AML Privacy/Security Officer has experienced training at various national level programs to ensure that the AMLMHBF is properly educated and is equipped to provide training to the remainder of the staff and board.

Copies of this and other policies and procedures will be given to employees directly engaged in the MHBF. Records regarding training, notification, privacy reminders etc will be maintained and kept on file for 6 years after they created.

A quick reference summary of training requirements follows:

<u>Who</u>	<u>What</u>
All AML employees	<ul style="list-style-type: none"> * General HIPPA rules / requirements / penalties * Periodic reminders (annual update & refresher)
MHBF staff	<ul style="list-style-type: none"> * General HIPPA rules / requirements / penalties * Periodic reminders (annual update & refresher) * In-depth initial training * Periodic updates (refreshers) * Bulletins re: new requirements (as needed)
New employees	<ul style="list-style-type: none"> * General HIPPA rules / requirements / penalties * Periodic reminders (annual update & refresher) * NON- MHBF – Handbook introduction * MHBF STAFF – Handbook introduction <ul style="list-style-type: none"> - Specific in-depth training first day
MHBF Board Members	<ul style="list-style-type: none"> * General HIPPA rules / requirements / penalties * Periodic reminders (annual update & refresher) * In-depth initial training * Special briefings for new Board Members as they are elected to serve.
Board of Directors and Management	<ul style="list-style-type: none"> * General HIPPA rules / requirements / penalties * Periodic reminders (annual update & refresher) * In-depth initial training

RECORD RETENTION: retain all records for 6 years period from date of creation.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Sanctions – Employee

Policy No. 6

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

The EDI requirements contained in the HIPAA regulations have highlighted and brought to the forefront the need to keep PHI private. Through specific privacy and security rules, every attempt has been made by the AML/MHBF to keep paperwork and electronic systems secure from unauthorized access.

AML/MHBF Policy & Procedure No. 4 points out that while technical controls are necessary, experience suggests that eighty percent (80%) of all controls should be related to behavioral safeguards. Behavioral safeguards are people related.

AML/MHBF employees have differing levels of involvement with the AML/MHBF and PHI. These levels range from minor involvement (telephone operators, financial, clerical, etc.) to maximum involvement (MHBF management, MHBF customer service operators, MHBF claims processors, etc.)

It is the intent of the AML/MHBF to provide adequate and appropriate training and education to each AML/MHBF staff member, based on their level of involvement in Fund operations, so that they can go about doing their work with full knowledge of HIPAA rules and regulations and their responsibility to protect PHI from unauthorized access, modification, or communication.

It is the policy of the AML/MHBF to deal with individual staff members who either intentionally or through carelessness allow PHI to be released or modified in an inappropriate manner. Both the severity of the violation and circumstances related to intent will be considered when determining the action(s) to be taken against the offending staff member. Possible punishments may include reprimands, suspensions or termination. Recommendations in each individual case, regarding punitive action will be made by the Chief Privacy Officer and Primary MHBF Supervisor(s) to the AML Executive Director, who will determine the final action to be taken. For further guidance on employee discipline, the AML Handbook should be consulted.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Patient Rights to Protected Health Information (PHI)

Policy No. 7

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

Before announcing patient's rights to their PHI, the definition of PHI should be revisited.

PHI is individually identifiable health information that is transmitted or maintained in any form, which identifies or could reasonably be used to identify the subject (member) of the information. PHI encompasses information, which may or may not include electronic information, paper records and oral communications. The exact form of the PHI is irrelevant.

Generally, individuals have a right to receive written notice of the AML/MHBF's privacy practices. This notification will be accomplished annually via distribution of the MHBF Booklet and the Policies & Procedures will be attached to the AML Website.

Members have the right to request certain restrictions on the use/disclosure of their PHI. However, not all member requests will/can be honored due to other disclosure obligations as listed in AML/MHBF Policies & Procedures No. 10 (consent and authorization requirements) and the practical necessities of processing claims.

Members have a right to access and review their PHI, with the primary exception of psychotherapy notes. The Fund can charge for costs incurred in providing copies of records, as well as set times and places for physical review. Patients have a right to seek amendments to PHI; however, the AML/MHBF is not obligated to comply with each request. Further, the AML/MHBF will verify changes with the MHBF Assistant Director before they are made.

Individual members also have a right to request and receive accounting for PHI disclosures made to individuals other than those involved with the proper business of the AML/MHBF.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Complaint Process

Policy No. 8

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

The Fund provides for essentially two tiers of complaint processes.

The first tier rests within the covered entity, AML/MHBF. The Fund has developed, and is providing, a process for individuals to make complaints concerning the Fund's policies and procedures and its compliance with such policies and procedures.

The Fund has appointed the Chief Privacy and Security Officer (CPSO) as the individual to receive all initial complaints. (See BELOW). The CPSO will receive, document and record all complaints, ensure investigation of the complaint, and decide and record their ultimate disposition. Further, the CPSO will keep both the AML Executive Director and the MHBF Board advised of all complaints and the ultimate disposition of each complaint. Policy No. 6 discusses sanctions imposed on individual staff members who violate any applicable regulations, policies, and procedures in conjunction with the AML Handbook.

The CPSO will ensure that the Fund mitigates, to the maximum extent possible, any harmful effects that may have resulted from the misuse of PHI. The CPSO will also ensure that no intimidating or retaliatory action will be taken or threatened against individuals exercising their right to complain.

The second tier open for complaints is to directly submit a complaint to the Federal Secretary of Health. An individual who believes the Fund has not complied with applicable requirements of HIPAA may file a complaint with the Secretary. The complaint must be written, either on paper or electronically, and it must be filed within one hundred eighty days (180) of when the complainant knew, or should have known, that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. All complaints must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation.

The Health Fund Chief Privacy and Security Officer will interface and cooperate with any Federal inquiry as required to ensure proper and timely resolution of such.

**HEALTH FUND CHIEF PRIVACY AND SECURITY OFFICER: DON MYERS
PHONE NO. (501) 374-3484, Ext. 101**

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Dealing with Business Associates

Policy No. 9

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

HIPAA regulations introduced and defined the concept of a BUSINESS ASSOCIATE. All “covered entities”, such as the AML/MHBF have occasion to do business with, and exchange PHI with, other business and non-covered entities during their normal course of business.

With respect to a covered entity, such as the AML/MHBF, a BUSINESS ASSOCIATE is defined as, a person who on behalf of such covered entity or of any organized health care arrangement in which the covered entity participates (other than in the capacity of a member of the workforce of such covered entity or arrangement) performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information (claim processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing) or provides (other than in the capacity of a member of the workforce of such covered entity) legal, actuarial, accounting, consulting, data aggregation, management, administration, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the services involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (SEE PAR 160.103 – General Administrative Requirements.)

BUSINESS ASSOCIATE AGREEMENTS – Each covered entity, including the AML/MHBF, is required to develop and obtain signed agreements with its non-covered Business Associates. The agreements much include language that obligates the Business Associate to protect, use and disclose PHI in accordance with the HIPAA rules and regulations. The essence of these requirements relate to: a) permitted uses and disclosures, b) required disclosures, and c) the minimum necessary disclosure standard. These requirements are spelled out in detail in AML/MHBF Policies and Procedures No. 10. Once agreements are in place, the covered entity still has some obligation to ensure the Business Associate remains in compliance with the terms of the agreement and the HIPAA regulations. While there is no audit like requirement, nor is a direct review/oversight required, a covered entity will not be considered in compliance with the standards in Paragraph 164.502, if the covered entity knew of a pattern of activity or practices of the Business Associate that constituted a material breach or violation of the Business Associate’s obligation under the contract or arrangement, unless the covered entity takes reasonable steps to cure the breach or end the violation, as applicable, and if such steps prove unsuccessful,

terminate the contract or arrangement, if feasible or if not feasible, report the problem to the Federal Secretary of Health.

Members of AML/MHBF general management and staff will be periodically reminded of their obligations regarding our Business Associates. (To identify new Business Associate Candidates and “monitor” existing agreements.) If any problems are detected, they will be referred to the Chief Privacy and Security Officer, who in turn will work with AML/MHBF management, and the Business Associate in question, in order to resolve the matter.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Consent & Authorization Requirement

Policy No. 10

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

As discussed in Policy No. 3, HIPAA works toward a MINIMUM NECESSARY approach to the use, disclosure, or requesting of PHI. As such, there are also strict rules and levels of disclosure to which AML/MHBF, as a covered entity, must comply with.

LEVELS OF PHI DISCLOSURE:

- A. Required – Individuals must be allowed access to their PHI, with the exception of psychotherapy notes. The Fund is also required to supply data as required by the Federal Department of Health & Human Services for compliance and enforcement purposes. See also Policy No. 7, Patient’s Rights to PHI.

- B. Permitted
 - 1. Uses and disclosures required by law
 - 2. Public health activities (i.e. vital statistics, communicable disease control, product recalls, etc.)
 - 3. Disclosures concerning victims of domestic violence or elder abuse
 - 4. Use and disclosure for health oversight activities (state licensure, DOJ, FDA, Medicaid)
 - 5. Judicial and administrative proceedings
 - 6. Law enforcement (court orders, subpoenas)
 - 7. Disclosures to coroners and medical examiners
 - 8. Organ procurement organizations
 - 9. Research purposes (with permission from an internal review board)
 - 10. Emergencies with serious threats to health or safety
 - 11. Specialized government functions (military)
 - 12. Workers’ compensation reviews (to the extent required by state law)

- D. Disclosures with permission of the covered, or subject, individual only - The AML/MHBF requires written consent to release data to any individual, other than the applicable member. This also pertains to discussions regarding any PHI with any source (except those listed in item B above, including municipal administrative staff.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Customer Service Guidelines (Phone inquiries)

Policy No. 11

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

This policy outlines approved methods used in determining the identity and relational status of various callers who seek information via the phone regarding PHI relative to one of the AML/MHBF members.

The procedure also outlines information that should and should not be given out, depending on the relationship of the inquiring person to the covered member.

First, in order to establish that the person making the phone inquiry has correctly identified themselves and/or their relationship to the covered client, customer service shall: determine if the call or inquiry by fax or e-mail is being presented by a provider, the employee/member, family member or other person. Guidelines relative to information that should or should not be given to various callers is as follows:

PROVIDERS

- Use either voice recognition or a call back procedure to ensure the validity of the person calling
 - Limit discussion to items necessary in order to determine proper payment for services

EMPLOYEE/MEMBERS

- Identify person by using Social Security Number, Group Number, or name and Date of Birth
- Provide information requested only...consult supervisor regarding any questionable data requirement

FAMILY/OTHER

- Must have approval of verified member...document approval...give minimal information only

(NOTE: most facsimile documents come directly to MHBF employees; however a few documents may initially come to the AML/MHBF receptionist for electronic distribution. The individual employed in this position is bound by the same policies, procedures and rules applicable to the AML/MHBF staff members and must not disclose PHI.)

DOCUMENTATION OF REQUESTS

- Record caller's name, phone number, member or relationship, Social Security Number, Group Number, and Date of Birth

ELECTRONIC DOCUMENT CAPABILITY

- The computer system will date stamp and identify data originator

INAPPROPRIATE CONTACTS

- Calls from City Clerks, unauthorized family members or others...can not discuss claims, diagnosis, or type of providers without express written consent for each and every individual contact. Discussion or release of data to persons other than the member him/her self is discouraged.

ONLY DISCLOSE NECESSARY PHI

- AML/MHBF staff will give out data only to specific answers to specific questions. Ancillary discussions relating to the member and their PHI is prohibited.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Electronic Data Interchange

Policy No. 12

Dates: Original 12/11/02 Latest Revision _____

Executive Approval: _____

To facilitate EDI between providers, the Fund, etc., the AML/MHBF has installed the “X-12” program to work with existing AML/MHBF claims processing programs. The “X-12” program utilizes the national standards for EDI codes and data sets.

The MHBF has initially chosen not to contract with a Health Care Clearing Houses at this time. Electronic claims will initially be handled via e-mail. As of November 2004, no provider has attempted to submit claims to the MHBF via any electronic mode.

The Fund has put necessary physical and administrative security measures in place to ensure protection of EDI transactions from unauthorized access. This process will be updated as time and circumstance change.

**ARKANSAS MUNICIPAL LEAGUE
MUNICIPAL HEALTH BENEFIT FUND**

POLICIES & PROCEDURES

Title: Protected Health Information Management and Storage

Policy No: 13

Dates: Original 12/11/02 Latest Revision _____

Executive Approval _____

All PHI, including electronic or paper documents obtained during the process of utilization review or bill auditing will be kept confidential in compliance with applicable federal, state, and local laws and regulations.

PHI is to be used solely for the purposes of utilization review, case management, quality assurance, discharge planning, and claims payment. Such information will be limited only to authorized individuals having the authority to receive the information in order to conduct utilization management and related processes.

The following shall apply:

1. Definition: PHI is individually identifiable health information that is transmitted or maintained in any form, which identifies or could reasonably be used to identify the subject of the information.
2. PHI encompasses information in any form, electronic or paper, that contains the member's name, social security number or any other element of information that might reasonably be used to identify the subject of the information.
3. Access to PHI is limited to those individuals who need such information to perform their specific and limited job responsibilities. As such, access to patient specific information is limited on a need to know basis. When contacting a doctor's office or hospital, the MHBF staff will provide a reference number, name and professional credentials to the designated utilization representative.
4. Confidential information will be released only to authorized parties in a manner consistent with applicable laws and regulations and AML/MHBF Policies and Procedures. MHBF employees will be required to consult their supervisor(s) as questions arise; in some cases, the issue may be referred to legal counsel for an opinion.
5. Physical Storage of PHI

- A. All such documents will be maintained only in designated staff work areas and secured at the end of the workday. Access to offices and work areas handling confidential documents will be limited to authorized staff.
- B. Confidential documents will not be taken home or otherwise removed from the office.
- C. When files are off-site (i.e. For Scanning purposes), AML/MHBF will contract to ensure that these facilities are kept locked when not in use and access will be limited only to authorized individuals.
- D. Physical access to the AML/MHBF building, or areas of the building, will be limited to authorized parties and controlled through a coded locking door system.

6. Electronic Storage of PHI

- A. Access to confidential information will be limited by password to the appropriate staff that utilizes such information to accomplish their job responsibilities.
- B. Passwords are assigned separately to appropriate staff members, and these passwords will not be shared with others. All passwords will be randomly chosen by the IT Department, and passwords will be changed on a regular basis.
- C. If a staff member leaves their desk for lunch, a meeting, or any other extended time frame, they will be required to ensure their individual computer is locked. A screen saver device is not considered adequate security to prevent unwanted access to a computer.
- D. E-mails containing PHI will be closely guarded and will be deleted when no longer needed to perform a necessary job function.
- E. The central computer equipment is safeguarded with a coded door locking system and a non-destructive fire suppression system.

7. Fax Sheet

- A. The confidentiality disclaimer will be used on all outgoing faxes, and no references to the individual member's name or other identifying information will be contained on the cover sheet.
- B. Staff members are directed to limit the amount of outgoing medical information to only that which is necessary to accomplish the purpose of the

fax and to send faxes only to individuals who are the designated party to receive such information.

- C. MHBF employees will be assigned direct fax numbers as needed so they can receive fax documents directly thus limiting the possible exposure of PHI to unauthorized personnel.
 - D. The AML/MHBF receptionist may receive occasional incoming fax documents, thus will be thoroughly trained regarding HIPAA privacy regulations and requirements.
 - E. Incoming faxes are subject to all policies noted herein.
8. Conversations regarding PHI should not take place in office space outside of designated areas or the building. This prohibition includes, but is not limited to, elevators, the lunchroom, hallways, restrooms, the parking lot, and administrative offices.
 9. When using telephonic communications, all staff members shall confirm that the other party is entitled to PHI. Confirmation shall occur as through the following of specific MHBF procedures, that may change periodically. (i.e.: Social Security Number, Date of Birth).
 10. Staff will not use cellular phones to conduct day-to-day operations.