SWMBH MI Health Link Operating Policy 7.1

Subject: ISM Data Storage, Retention and Maintenance	**Accountability:** Information Technology	**Effective Date:** 1/1/2014	Pages: 2
REQUIRED BY: BBA Section 164.308 Administrative Safeguards PIHP Contract Section NCQA/URAC Standard SASARF Other		Last Reviewed Date: 8/4/16	Past Reviewed Dates: 1/1/14
LINE OF BUSINESS: Specialty Waiver (B/C) I Waiver ABW Waiver SUD Medicaid SUD CA Block Grant MME OTHER:	**APPLICATION:** SWMBH Staff and Operations Participant CMHSPs SUD Providers MH/DD providers DD providers MME providers Other:	Last Revised Date:	Past Revised Dates:
Approved By: Date: August 4, 2016		Required Reviewer: Chief Information Officer	

I. Purpose

To establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

II. Policy

This policy provides information for management and workforce members for performing periodic computer system backups and to ensure that critical data is adequately stored, retained and protected against loss and destruction.

III. Standards and Guidelines

A. HIPAA-compliant Data Center host vendor has been selected: Information Technology Partners (ITP)

1. Backup Schedule
   a. Backup schedule will be identified based on host vendor capabilities and offerings.

B. Length of Data Retention

1 Full system backups should be copied and/or archived and not be stored in the same geographic location as the source systems.

2 Archived backups must be periodically tested to ensure that they are recoverable.

3 All electronic data shall be retained at least as long as required by the Michigan Records Retention and Disposal General Schedule #20, State and Federal law and regulations and Southwest Michigan Behavioral Health (SWMBH) policies and procedures.

C. Physical Access Controls and Security

1 The minimum acceptable level of physical security for any backup system or server(s) is to place it behind a locked door to which access is controlled by the SWMBH Security Officer (as identified by

the SWMBH Executive Officer).

2. Physical access to backup equipment or software shall be approved only to those with appropriate credentials and abilities and must be approved by the SWMBH Security Officer.
3. Staff that is afforded security access to locked rooms or safe combinations for the purpose of retaining backup information shall be responsible for safeguarding keys, key codes or combinations.
4. Any staff that should inappropriately share their access to backup equipment or software will be subject to disciplinary action, up to and including termination of employment.

D. Testing

1. Testing schedule will be identified based on host vendor capabilities and offerings.

IV. Definitions

Protected Health Information

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

V. References

BBA Section 164.308 (a) (7)

VI. Attachments

None