HARDIN COUNTY
Risk Analysis, Data Disaster Recovery and Emergency Mode Operations

DATA SERVICES: *Community Services*
LOCATION: *Community Services Office*

I. LIST OF ALL Electronic Protected Health INFORMATION (EPHI)

Repository Inventory and Risk and Criticality Assessment	1	2
Repository Name	MHIS	Client Data - Server
Custodian Name	Adams	Jones
Custodian Contact Information Phone	641-456-2128	641-373-6445
Custodian Contact Information Address	1201 14th Avenue	1215 Edgington Ave
System Name	Clients	SERVERS
System Location	Annex	Law Enforcement Center
System Manager Contact Information Phone	641-456-2128	641-939-8125
Number of Users that access the repository	9	9
Number of Records	0	Thousands
Risk Level (Low<users<records; High>users>records OR Critical; else Medium)	Low	Low
IF "Medium" or "High" is a Data backup Plan in place?	Yes	Yes
Dates to test backups	As Needed	Daily
Criticality Level (High or Low)	Low	Low
IF "High" is a Disaster Recovery Plan in place?	No	Yes
Dates to test recovery		Daily
IF "High" is an Emergency Mode Operations Plan in place?	Yes	Yes
Dates to test emergency mode	9/30/2019	9/30/2019
Dates to re-review inventory and assessment	6/30/2020	6/30/2020
FIREWALL used that meets guidelines?	Yes	Yes

In addition, all staff have access to the Community Services Network (CSN) which is a web based consumer data system. A copy of the emergency data recovery plan for CSN is kept on sight in the Community services office.
Equipment Insured by: Heartland Risk Insurance Pool 515-727-9344
Insurance documents are stored: Printed copy in Auditor's office.

II. RISK ANALYSIS See above

III. BUSINESS IMPACT ANALYSIS

Costs of Loss of EPHI: The cost of recreating the EPHI is minimized by the availability of nightly full backups completed on the SERVER. In the event of loss of any of the servers, we can reload the information from the backups. In the worst case, if the destruction occurred at the end of the day, we would have to re-key just that day's transactions. During the busiest time of the year, that would require two person-days of effort. If EPHI is lost, the exposure would be in terms of damage to the reputation of the county and possible failure to provide services. In addition, there is the possibility of costs associated with legal actions.

Risks: The risk of physical loss of information, both critical and sensitive, is associated with the reliability of the equipment, the power protection afforded the equipment, the security of the premises, and the age of the equipment. We have tried to minimize these risks by the following:

1. Adequate Uninterruptible Power Supplies, and associated power protection is provided for each machine;
2. The quality of the equipment is reasonable, within budget constraints;
3. The premises are protected with high-quality locks with copy-protected keys, fire protection, and fire detection systems. All servers are located in a secure environment.
4. Any Electronic Protected Health Information that is removed from the office is backed up on the server before being removed from the office.

IV. SECURITY SAFEGUARDS
All personnel are made familiar with the requirements for security and confidentiality through training.

A. Backups:
Full backups Monday thru Friday after normal business hours. They are stored in an encrypted network attached storage device in the Hardin County Law Enforcement Center. This information is backed up multiple times per day off site to a server in Des Moines.

B. Paper forms used for data input, and reports associated with confidential information are kept in files which are locked when we are away from our offices. The building is kept locked after normal work hours, on weekends and holidays, and during periods when staff are absent from the office area. All computers in the office are password-protected and have inactive-lock time-out software installed.

C. Access to EPHI is limited to the appropriate personnel. A list of data access privileges for each job description is as follows:

Director: Access to all files.
General Assistance: Access to all files.
Service Coordinators: Access to CSN and Service Coordinator information.

Master passwords are only known by the IT Director, Network Engineer, and the Director, and all passwords are changed on a 90 day cycle or more frequently if a breach of security is suspected, or the employee or their supervisor or the Department Head leaves county employment.

D. The disaster recovery plan, security safeguards, access rights, and staff responsibilities are covered in our HIPAA Compliance Plan. This Plan is reviewed yearly and updated as required. Employees in this department are cross trained and are given access to all data, however employees will not access data unless it is necessary for them to conduct their duties. All persons will be required to use a Unique ID and password meeting the minimum standards in order to access systems containing EPHI. The network is configured to force the expiration and changing of all passwords at least every ninety (90) days.

E. Employee security:

- No employee is to bring to work any unauthorized data storage device such as USB memory keys, external plug-in storage media such as hard disk drives, 'Zip' drives, or CD burners. Breaches of this rule will result in sanctions outlined in the HIPAA Compliance Plan up to and possibly including immediate dismissal.
- All electronic communications that contain sensitive data must be password protected or encrypted.
- As soon as an employee is dismissed or resigns, the employee's access to data is terminated.
- No employee may give their passwords to any other employee (apart from hard coded passwords to the Administrator), or use any other employee's passwords to gain access to data for which they should not have access rights.

F. Equipment Auditing:
The Auditor will maintain and manage an active inventory of all equipment and software located in the Department. Copies are located on the server. All incoming equipment and software will be labeled and tracked for identification purposes when it enters the company.

G. Data Auditing:
Internal audit procedures have been implemented to regularly review records of information system activity, including audit logs, access reports, and security incident tracking reports.

1) An internal audit procedure has been established and implemented by this Department to regularly review records of system activity. The internal audit procedure utilizes audit logs, activity reports, and other mechanisms to document and manage system activity.
2) Audit logs, activity reports, and other mechanisms to document and manage system activity are reviewed at intervals commensurate with the associated risk of the information system or the EPHI repositories contained on said information system.
3) The Audit Control and Review Plan includes the following procedures:
   a) Systems and Applications to be logged: COMIS and Client Data Files.
   b) Information to be logged for each system: Each system's audit log includes; User ID, Login Date/Time, and Activity Time. Audit logs will include semi-annual review of employee's current data access for twenty minutes, i.e. employees will be contacted every six months to log access and modifications to any EPHI Files for the next twenty minutes.
   c) The following procedures to review all audit logs and activity reports will be followed: Semi-annual audit reports will be reviewed and stored for six years by the Department. The interval of the system activity review does not exceed, but may be less than, one hundred eighty (180) days.
4) Security incidents such as activity exceptions and unauthorized access attempts if they occur are detected, logged and reported immediately to the Assistant Director and the HIPAA Security Officer.

V. PLAN ACCURACY: This plan is tested and reviewed yearly and updated as required. All backup procedures are tested annually. Backup equipment is tested and serviced annually.

VI. Contact Data of Key Personnel The following employees' data is kept on file by the Department Head, and copies kept at home by each of the other key personnel.

Name: Linn Adams, AGENCY DIRECTOR
Cell Phone: 641-373-3341
E-mail: linn.adams@cicsmhds.org

Name: Micah Cutler, IT/GIS DIRECTOR
Cell Phone: 515-999-0294
E-mail: mcutler@hardincountyia.gov
Other contact: Courthouse: 641-939-8124

Name: Matt Jones, NETWORK ENGINEER
Cell Phone: 641-373-6445
E-mail: mjones@hardincountyia.gov
Other contact: Courthouse: 641-939-8125

Name: Carol Haywood, OFFICE MANAGER
E-mail: Carol.haywood@cicsmhds.org

Name: Jodi Hamilton, SERVICE COORDINATOR
E-mail: Jodi.hamilton@cicsmhds.org

Name: Mary Swartz, MENTAL HEALTH ADVOCATE
E-mail: mary.swartz@cicsmhds.org

Name: Mary Nelson, CLUBHOUSE COORDINATOR
Email: fiafc@hardincountyia.gov
Phone: 641-648-7500

Name: Kathy Vitasek, CLUBHOUSE ASSISTANT

In the event of change to key personnel (death, disappearance, dismissal, serious injury):
Department Head: The Service Coordinator Specialist is to immediately assume the temporary role of Department Head until a new Department head is appointed by the Board. System passwords may be changed by the appropriate IT personnel.

In the event of change to other key personnel, the Department Head will take appropriate action to assure duties are completed.

VII. ESSENTIAL SYSTEM INFORMATION
Backup drive type: HP Lefthand iSCSI
Backup software needed for data recovery: Veeam
Server configuration: Windows Server 2012 Standard Edition.
Workstation software: Basic configuration: Windows 7 Professional, MS Office 365 (at least 1 copy of Access).

VIII. EMERGENCY PROCEDURES:
A copy of these procedures is included with the employee manual. These procedures are described in the training of all new staff, and reinforced periodically to existing staff.

In the case of Natural Disaster or Fire:
- The **Director** should, as far as conditions allow:
1) Activate fire or tornado alarms manually, if they have not already been activated if applicable.
2) Notify the fire department (Phone 911). If the agency telephone system has been disrupted by the fire, etc, utilize a staff member's personal cell phone.
3) Shut down the file servers and eject the removable hard disk drives. All removable hard drives should be packed in the provided case and taken from the building. etc.
- **Department Head** should, as far as conditions allow:
Check all work areas and evacuate all staff. etc.
- **Other Employees** should, as far as conditions allow:
In the case of a fire, all employees should immediately leave their offices, closing their doors behind them, exiting the building at the labeled exits and meeting across the street on the South side of the Courthouse. If inclement weather staff should meet in the entryway of the Hardin County Sheriff's Office.

In the case of a tornado all employees will leave their office and go to the basement until an all clear is announced.

In the case of server failure:
Hardin County IT Director or his/her designee will:
1) Attempt all appropriate quick measures to bring the server back online.
2) Contact the supplier of the server to arrange an emergency replacement machine.
3) Acquire the most recent backup from the Department Head.
4) Restore backed-up data, as far as possible, to the server.
5) Organize the re-entry of data entered between the last backup and the installation of the new server.
6) Bring the new server online.
7) Have the failed server repaired or replaced.

IX. Emergency Mode Operations.
If Community Services becomes inoperable for a period of time, staff will be relocated according to the Hardin County Emergency Operations Plan. The IT Director or his/her designee will coordinate the replacing of IT equipment and restoring or accessing servers from the backup locations until services can be restored here.

Document last updated: *6/05/2018*

Passed and approved this 12th day of June, 2019.

_____
Reneé McClellan, Chairman
Hardin County Board of Supervisors

ATTEST:

_____
Jessica Lara, Auditor