Policy Number: HC-23	Page: 1	Of: 2
Title: Data Backup		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) DATA BACKUP

The HIPAA Privacy/Security Officer will insure that a robust data backup regimen is in place and operational at all times. The HIPAA Privacy/Security Officer shall personally insure that the procedures below are consistently maintained.

Audience

HIPAA Privacy/Security Officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.308(a)(7)

1) **Data Criticality Analysis**. A Data Criticality Analysis shall be performed and updated as appropriate. The backup regimen must be developed in a manner consistent with the data criticality.
1) **Multiple Backup Generations**. Backups should include as many generations as is practical to store. One backup per day is appropriate.
2) **Backup Software**. Appropriate backup software shall be maintained, with appropriate scripting. These scripts shall be reviewed and adjusted as appropriate whenever hardware or software upgrades are performed to insure that appropriate data backup is maintained.
3) **Off-site storage**. Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include an off-site backup, that is, in a separate facility from the one containing the physical hardware.
4) **Backup Documentation**.
   a) A written description of the backup regimen must be maintained, including a description of the backup software utilized, the backup method used (e.g. full system or incremental), details of the generations maintained, naming conventions used, names of backup scripts, and other information necessary to understand the backup strategy.
   b) User documentation, for use by a system administrator, shall be maintained to allow for an alternate person to verify the daily operation of the backup.
5) **Responsibility**. The HIPAA Security Officer shall designate the employee with primary responsibility to personally handle the backup. In the event that he/she is absent from

work, an alternate individual shall be responsible. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.

6) **Backup Log**. A daily written log shall be maintained documenting the date, person, verification that backup was completed successfully, and any comments. Problems should be immediately reported to the HIPAA Security Officer, or if the HIPAA Security Officer is away from the office, to the superintendent.
7) **Backup Media Security**. Backup media shall be maintained in a secure location.
8) **Testing and Plan Revision.** REVIEW AND UPDATE OF THE DATA BACKUP PLAN SHOULD BE CONDUCTED WITH ANY SIGNIFICANT UPDATE OF THE TECHNICAL ENVIRONMENT. On at least a quarterly basis, a trial restore shall be performed from the backup to verify the proper function of the backup process. Based on the results of this test, and any other environmental changes, the Data Backup Policy and Disaster Recovery Plan shall be updated. The results of this process should be documented and maintained for 1 year.
9) **Data Recovery Plan.** The HIPAA Security Officer shall maintain a written plan for restoration of data in the event of various system failures.