

CFR Part 164.312 section C (2), relating to the implementation specification for the Mechanism to Authenticate Electronic Protected Health Information (EPHI); is an addressable item under the current Health Information Portability and Accountability Act (HIPAA). This relates to data at rest and states the following:

“Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

The Department of Health and Human Resources(DHHR) Office of Management Information Services(OMIS), after careful assessment and consideration, has decided that to serve as our implementation of CFR Part 164.312 section C(2) we will use the following several resources:

1. All systems containing EPHI are backed up according to established policies and procedures. The applications that perform these activities are configured, as part of the verification process; to compare the completed back up files to the existing data as it resides on the target system.
2. The OMIS network is by definition a Private Network, secured behind dual proprietary firewalls.
3. OMIS has several additional layers of security in place including Access Control Lists at the router level as appropriate; Operating System based system logging and internal audit controls.
4. All applications containing Electronic Protected Health Information (EPHI) are required to have individual unique User ID's and passwords.
5. We are already addressing CFR Part 164.308(Administrative Safeguards) section 5(C), relating to Login Monitoring; which states that procedures must be in place for monitoring log-in attempts and reporting discrepancies. This has been implemented on both the application and the network level, and includes at a minimum the ability to record attempted log-ons' and log-offs. This captures successful and unsuccessful attempts.

By utilizing the comparison the verification of backup images (which serve as a reference), the multiple audit logging functions within DHHR and the use of individual and unique User ID's we can as needed reactively work to assure that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Based upon these factors we have determined that the above listed mechanisms already in place, taken together with a separate documented initiative to use each collectively; provides adequate and reasonable compliance with CFR Part 164.312 section C (2).