Sterling Seacrest Pritchard

BACKING UP MEDICAL RECORDS

HIPAA requires you to implement:

- **e-PHI copying procedures.** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
- **Restoration procedures.** Establish (and implement as needed) procedures to restore any loss of data.
- **Business continuation procedures.** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
- **Testing.** Implement procedures for periodic testing and revision of contingency plans.
- **Evaluation.** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

First steps toward compliance:

1) Perform a risk assessment to determine what electronic protected health information (e-PHI) you have and where it is located.
2) For the e-PHI in No. 1, determine what is currently being backed up, how it is backed up, and where it is stored.
3) Identify who is responsible for ensuring that exact, retrievable copies of backup data are made. [You may be outsourcing this to a third-party vendor]
4) Develop a backup schedule which identifies what servers are backed up and the schedule for backup (e.g., hourly, daily, weekly, monthly, or annually). For EHRs, backups four times per day is best practice. Internal file servers utilized by staff should be backed up every hour.
5) Document the type of backup required (e.g., incremental, full, or one-time).
6) Document the level of backup (e.g., File Level – uploading essential files and folders to the backup storage; Virtual Machine level; or Application-level backup).
7) Automate the data backup plan but have it monitored by support staff for incidents such as a failure or a missed backup with detailed reporting enabled.
8) Encrypt your backed up data both while in rest and in transit, and protect it with MFA and a rigid access control list (ACL), i.e., a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. ACLs can also be installed in routers or switches, where they act as filters, managing which traffic can access the network.
9) Develop a comprehensive backup policy that addresses all of the above as well as the restoration process.
10) Testing the data backup plan every six months and document concerns and issues along with a plan to address same.

Please Note: SSP is not a law firm, and our recommendations should not be construed as, nor are they intended to be, legal advice. SSP encourages its clients to consult with legal counsel and/or other professionals about the information contained in this communication.

2024 © Sterling Seacrest Pritchard, Inc. | sspins.com