

Our Commitment to You

City Wide Data Storage is dedicated to helping our customers meet the needs of their customers. In the information world this often means that our customers are given a set of requirements valued by their customer. In many cases adherence to these requirements comes in the form of the certification or compliance to an industry guideline. Our intent is to consistently be in step with our customer's needs in this area, thus we attempt to give our customers information about how the use of City Wide Data Storage service meets these guidelines. Each section on this page will address a different set of requirements. If you have questions about a requirement that is not listed here, please contact us at City Wide Data Storage. We will make every attempt to provide you with the information necessary to assist you in meeting your business needs.

HIPAA – Health Insurance Portability and Accountability Act (Congress 1996)

Information – <http://www.cms.hhs.gov/HIPAAGenInfo>

Section – 164.308(a) (7) (i) – CONTINGENCY PLAN

Requirement – Establish a contingency plan for responding to requests for information in case of emergency or other occurrence (i.e. fire, vandalism, system failure, or natural disaster) that damages systems containing electronically protected health information.

City Wide Data Storage Proposition – City Wide Data Storage online backup service provides a secure offsite location for the storage and recovery of our customer's data from anywhere in the world.

Section – 164.312 (a) (1) – ACCESS CONTROL

Requirement – Implement policies to restrict the access of the electronically protected health information to those persons or software programs that have been granted access rights.

City Wide Data Storage Value Proposition – All access to backup files is restricted to an authorized user name and password. In addition, a second level of protection is provided since the information contained in any backup file remains encrypted while stored on City Wide Data Storage redundant hardware. These files are password protected and can only be decrypted by a person using this password.

Section – 164.312 (b) (1) – AUDIT CONTROL

Requirement – Implement policies required to record and examine activities on systems containing electronically protected health information.

City Wide Data Storage Value Proposition – Automated use of City Wide Data Storage backup service ensures an accurate audit trail of changes made to health information contained on your system. City Wide Data Storage also monitors and notifies our customer of any failure in the backup systems which might require attention. Attention to this detail allows our customers the ability to detect failures before an issue arises.

Section – 164.312 (c) (1) – DATA INTEGRITY

Requirement – Implement policies to protect electronically protected health information from the improper alterations or destruction.

City Wide Data Storage Value Proposition – Our systems use the latest technology to verify that what is sent to our backup servers is an exact copy of what our customers send. Our retention feature ensures that this data is accurately and efficiently archived for point in time retrieval based on our customer's backup policies. The data is maintained in three places and accessible from one of two highly available locations. The third location is our backup of your backup. This provides a level of protection against destruction that effectively meets this requirement.

Section – 164.312 (d) (1) – IDENTITY AUTHENTICATION

Requirement – Implement policies that verify the identity of a person seeking access to electronically protected health information.

City Wide Data Storage Value Proposition – Access to all City Wide Data Storage files and account information is restricted to an authorized user name and password.

Quotes from Tech Republic on HIPAA recovery regulations:

HIPAA doesn't spell out what these measures are, but it does note that failure to adequately recover from a disaster could lead to noncompliance.

You'll notice that peppered throughout the final HIPAA rule are references to NIST documents. The NIST 800 series of documents provide guidance for compliance with federally mandated regulations.

[EDITOR'S NOTE: NIST stands for the National Institute of Standards and Technology. Check out their Web site at <http://www.nist.gov>.]

There are three things about data that come into play under HIPAA: integrity, availability, and confidentiality.

In a weather or national security emergency, information that can be restored seamlessly to a point in time may make the difference in an effective health care delivery system.

The person that validates the successful restore should not be the person that performs backups.

You've got to establish and enforce a mechanism that correctly receipts what media leaves your facility and what is stored at your offsite storage facility. You should periodically review contractual agreements for offsite storage and follow up to inspect offsite storage to validate that secure and environmentally controlled off-site storage meets your needs.

And here's my summary in a nutshell. If you are already taking the "bare-bones" steps I've mentioned, you will need to "prove it."

Do my procedures adequately answer by whom, what, when, where and how my policies were implemented?

Construct a checklist for your procedures and ensure that it is in use.