

## **OnlineBackupVault.Com**

Is your one source for a complete reliable backup system. OnlineBackupVault.com has multiple servers with multiple power sources and multiple connections to the Internet to ensure reliability and helping to ensure that your data will be available in the event of catastrophe. We built our system to be completely encrypted and secure. All encryption is done on the LOCAL PC, meaning the machine that stores the initial information. When the data leaves your server/pc it is encrypted with the password that you set, when it reaches our servers, the data is meaningless to anyone without the password that only YOU know. When the software is downloaded in the case of a restore, the encryption key (password) is REQUIRED so that you can decrypt the restore. Only YOU have access to the encryption keys, from the server level the data is meaningless without the key. You can rest assured that your data is secure and backed up in multiple locations.

## **HIPPA, PRIVACY AND SOX Compliance**

Information about regulatory compliance as it relates to HIPAA, SEC/NASD, and Sarbanes-Oxley can be found below.

Health Insurance Portability and Accountability Act (HIPAA)

Requirement: Electronic personal health information (ePHI) must be protected against any reasonably anticipated threats or hazards.

What we do: The data is housed in two separate data centers. Both the primary center and the secondary remote center are heavily secured. Redundant fail-safe systems protect the data in every step of the backup and storage process.

Requirement: Access to ePHI must be protected against any reasonably anticipated uses or disclosures that are not permitted or required by the Privacy Rule.

What we do: The data is encrypted before transmission and is always maintained in encrypted state. Access is restricted by password authentication.

Requirement: Maintenance of record of access authorizations.

What we do: Access to data is date and time-stamped by user, providing a clear audit trail.

Requirement: If the data is processed through a third party (OnlineBackupVault.Com IT), entities are required to enter into a chain of trust partner agreement.

What we do: OnlineBackupVault.Com IT enters into a Business Associate Agreement with client, in which the parties agree to electronically exchange data and to protect the transmitted data. The Agreement states that the receiver of data (OnlineBackupVault.Com IT) is required to maintain the integrity and confidentiality of the transmitted information.

About HIPAA

The Health Insurance Portability and Accountability Act of 1996 imposes standards for the privacy and protection of all health information that can be linked to individuals. Health and Human Services (HHS) has published final HIPAA regulations that affect virtually every area of health-related organizations in the United States, from the one-physician office to hospitals, health systems, HMOs, health care support services, and others. Part of this act is focused on the secure storage and transmission of confidential patient data over computer networks. Privacy regulations were released in December 2000, made final on April 14, 2001, and went into effect in April 2003.

Non-compliance carries stiff civil and criminal penalties.

All health care organizations are affected in some way by HIPAA. The entities that are affected include all health care providers (even one-physician offices), health plans, employers, public health authorities, hospitals, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.

A broad definition of personal health information (PHI) includes - All individually identifiable health information in ANY form or media including subsets of health information such as demographics. The HIPAA privacy mandate defines who is authorized to access information (the right of individuals to keep information about themselves from being disclosed). HIPAA requires the ability to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of the information.

Healthcare organizations are required to individually assess their security and privacy requirements and take suitable measures to implement electronic data protection (both while in transit and during storage).

If the data is processed through a third party (OnlineBackupVault.Com IT), entities are required to enter into a chain of trust partner agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver of data are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information.

SEC/NASD

Requirement: Preserve the records exclusively in a non-rewriteable, non-erasable format.

What we do: OnlineBackupVault.Com IT preserves the records exclusively in a non-rewriteable, non-erasable format.

Requirement: Verify automatically the quality and accuracy of the storage media recording process.

What we do: The data is verified automatically every time a backup takes place.

Requirement: Serialize the original, and, if applicable, duplicate units of the storage media, and time-date for the required period of retention the information placed on such electronic storage media.

What we do: Even if data is restored to the client system, the original remains in the vault in the same exact state as the initial backup until it is cycled off at the end of the period chosen (whether that period is a day or 7 years).

The OnlineBackupVault.Com IT automated process and subsequent detailed reporting gives regulators a clear idea of the chain of custody of the stored information and also rapid access, should it be required.

All access to the stored data is documented and time/date stamped.

Requirement: Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable.

What we do: The data is available for online restores 24/7, 365 days a year.

All backups are stored with the catalogs (indexes) and accessible to authorized users at all times.

Requirement: Store separately from the original a duplicate copy of the record stored on any medium acceptable for the time required.

What we do: OnlineBackupVault.Com IT online backup uses a process that backs up the original and duplicates it to a remote location. This is not a "mirrored" process, but a process that insures that the original data and any duplicate copies are identical. The data is stored on fault-tolerant disk media.

About SEC/NASD Regulations

In 1934, to protect investors from fraudulent or misleading claims in the securities industry, the SEC enacted the Securities Exchange Act, a set of laws that required records be made and kept for the purposes of review and auditing of securities transactions. In 1997, the Commission amended the primary rule 17a-4 to allow brokers and dealers to store records electronically. The SEC defines strict requirements for storage of these electronic records as detailed in its Rule 17a-4 and in NASD Rule 3010/3110.

The rules, effective as of May 12, 2003, apply to many types of records, including financial accounting documents, all communications received and all communications sent. The OnlineBackupVault.Com IT service enables clients to meet or exceed SEC and NASD regulatory compliance in regard to the preservation of financial records and electronic communications.

Requirement: Information cannot be tampered with or altered by any employee.

What we do: Data is always encrypted with 128-bit encryption, and OnlineBackupVault.Com IT does not have access to the password.

Requirement: Trail of transactions must be discernable and kept in sequence.

What we do: All iterations of a document are serialized, not overwritten.

Requirement: Audit trails

What we do: Access is date and time-stamped by user each time a document is accessed.

Requirement: Information is available only to client's authorized personnel.

What we do: Client access is only through authorized personnel with the password.

Requirement: Records must be accessible.

What we do: All backups are immediately available 24/7.

Requirement: Certain data must be maintained for not less than 7 years.

What we do: Data will remain in the OnlineBackupVault.Com IT vaults for as long as the client chooses to retain it. Retention is set during configuration, so once configured, the data is automatically stored for that period.

The Sarbanes-Oxley Act (SOX) of 2002 is one of the most important laws impacting public corporations to be passed in many years. The purpose of SOX is to protect investors from a continuation of the many accounting scandals over the past decade. The SOX places the onus on companies and registered accounting firms to comply with stringent rules regarding the accuracy and reliability of specific information by strengthening maintenance requirements of records, and the auditing/reporting of these records. Some of the provisions of the Act define what must be maintained, how long relevant material must be maintained, accounting procedures requirements, and consequences (criminal and civil) for failure to follow the Act. (There is no specific language about the mechanism or method of storing information in the Act). In placing a more rigorous requirement on financial reports the storing of the records becomes vitally important because the trail of transactions must be secure. The regulated companies in choosing a storage method will therefore look to a format that will insure it can satisfy the legal requirements of the SOX, in other words, the increased use of online remote data storage facilities/programs. Since an online computer data storage facility is not privy to the contents of the information it stores for a client, the facility is not responsible for ensuring that its customer is in compliance with what is being kept or who in the company (including independent auditors) has access; but is accountable for the availability and security of the information being stored. The online computer data storage facility must have safe guards in place to ensure quality control standards include the following:

- That information stored cannot be tampered with (altered) by any employee;

- That the client can ascertain when the information was created; (The records kept must allow a trail of transactions to be discernable so that ongoing transactions are kept in sequence.). That safeguard is in place to ensure that information is available only to the client's authorized personnel; That records are accessible whenever needed; and

- That the facility has the ability to maintain the data for the period stated in the Act. (Section 103 (a) (2) (A) (i): audit work papers and other information relating to any audit report is to be kept for a period not less than 7 years.