Data Backup Regulatory Compliance

Information about regulatory compliance as it relates to HIPPA, SEC/NASD, and Sarbarnes-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.

About HIPPA

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).

SEC/NASD

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

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

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. 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.

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.

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 Technics One LLC service enables clients to meet or exceed SEC and NASD regulatory compliance in regard to the preservation of financial records and electronic communications.

Sarbarnes-Oxley Act (SOX)

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

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

Requirement: Audit trails

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

Requirement: Records must be accessible.

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

About SOX

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 rating to any audit report is to be kept for a period not less than 7 years).