LiveVault Helps Make Healthcare Providers HIPAA Compliant

Regulation Name and Description: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT of 1996 (HIPAA) (a.k.a. Public Law 104-191)

TITLE I--HEALTH CARE ACCESS, PORTABILITY, AND RENEWABILITY

TITLE II--PREVENTING HEALTH CARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM

Industry Affected: Health Care, the term "covered entity'' is defined at Sec. 160.103 as one of the following: (1) a health plan; (2) a health care clearinghouse; (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by part 162 of title 45 of the Code of Federal Regulations (CFR).

Compliance and Enforcement: Federal mandate, not to supercede more stringent contrary state laws. Compulsory, with compliance deadlines. Fines and penalties for non-compliance (1st fine $50,000, 2nd fine $200,000, liability if violation occurs and healthcare provider found not in compliance; fines of $100 per record that has been compromised; non-compliance could jeopardize healthcare provider as an going concern).

Important Dates: Compliance with transactional code set standard was required by October 15, 2002; compliance with privacy ruling including compliant backup methodology was required by April 14, 2003 for majority of covered entities with an extra year grace period for small health care providers (April 14, 2004); compliance with security provision final ruling including compliant backup methodology is required by April 21, 2005 with an additional one year grace period for small plans, defined at 45 CFR 160.103 as health plans with annual receipts of $5 million or less.

Overview: HIPAA has multiple requirements to improve the access and portability of patient health records while maintaining strict privacy and security. The law is supplemented by standards in the form of "final rulings" that codify how health care providers and those that handle individually identifiable patient health records must comply. The security and privacy rulings include provisions that require compliant backup methodologies to insure that individually identifiable health records remain private and secure. The security and privacy rulings require a backup plan, a disaster recovery plan and an emergency mode operation plan (Section 164.308).

Key Messages:

The LiveVault Online Backup and Recovery Service (the Service) provides critical data security protection without compromising patient privacy that helps you meet or exceed HIPAA regulations.

LiveVault Fulfills Key Security Needs

Health care providers are required to implement comprehensive security systems to ensure that electronic patient records are protected against data loss and unauthorized access. A HIPAA-compliant security system needs to include a combination of administrative procedures, physical safeguards, and technical measures to protect patient information while it is stored and while it is transmitted across communications networks.

The LiveVault Service implements security and data availability features in each of these areas:

- ✓ Easy, frequent data backups preserve a retrievable, physically secure, off-site, exact copy of patient records. All data is encrypted before it leaves the customer's server and remains encrypted during transmission and storage. Only the customer has access to the password.
- ✓ Backup transmissions are further protected by integrity controls, mutual authentication, access controls, alarms for abnormalities, auditing of failed logins, and event reporting.
- ✓ Disaster recovery is made easier with tools to quickly restore lost data and servers.
- ✓ "Media control" risks are reduced compared to traditional disk or tape backup techniques by eliminating insecure methods of data handling, especially the transporting of media offsite.
- ✓ The LiveVault Service offers multiple "point in time" backups per day – as often as every 15 minutes – to insure that recovery is possible from corruption events with minimal data loss.
- ✓ The LiveVault Service retains historical backups for as long as 7 years.

LiveVault Meets Privacy Requirements

Under the HIPAA health data privacy rules, health care providers that engage in electronic transactions must observe privacy safeguards to restrict the use and disclosure of individually identifiable health information. As independent third-party service providers, LiveVault and LiveVault's agents and subcontractors are "business associates" under the HIPAA security and privacy rules. If needed, LiveVault will provide and sign a business associates agreement in conjunction with use of the LiveVault Service.

LiveVault and its agents do not receive data for any purpose except to provide data restoration as insurance against data loss. Because the data is encrypted before it leaves the customer's server and only the customer has access to the password, LiveVault and its agents cannot access the data.

LiveVault Is An Important Part Of Your HIPAA Compliant Solution

Preventing Unauthorized Access.

- *Secure Transmission and Storage:* Customers' data is encrypted with 256-bit AES encryption and then transmitted and stored as encrypted data at vaults that reside offsite at a secure remote facility. Customer's encrypted data may also optionally be stored on an appliance at the customer's site to facilitate rapid restores.
- *Logical Access*: Logical access to the data is strictly controlled, with a secure user interface that does not permit a user to view the contents of data. Furthermore, data can only be restored to the server where the data originated, or to a server where the data encryption key has been locally installed. (The user interface cannot be used to specify, change, transport or access data encryption keys.)

Preventing Loss of Data.

- *Physical Controls:* The data center is a hardened facility meeting numerous physical criteria. Exterior walls are double reinforced concrete. Access is strictly controlled through administrative procedures, physical safeguards, and technical security measures.
- *Redundant Vaults:* All backed up data is stored on two separate (redundant) vaults. The data center has redundant bandwidth providers, power, and HVAC.
- *Retention For Up To 7 Years.* Historical backups can be retained for up to 7 years.