



## **Mirrored Storage, Inc.**

### **Data Backup and Compliance Legislation - HIPAA**

White Paper presented by:

**Mirrored Storage, Inc.**

**ONLINE BACKUP SOFTWARE**

<http://MirroredStorage.com>

#### **Introduction**

The amount of data used by today's businesses has increased exponentially from just five years ago. Corporate scandal, international unrest, and glaring security flaws in computer operating systems and software applications have resulted in a much more intense and detailed analysis of data as it enters and leaves the enterprise. Fortune 500 companies have been vilified in the press for reckless data stewardship, and in some cases of outright fabrication of financial and performance reports. In extreme cases, executives are now lounging in Federal facilities, denying to the bitter end that they had any knowledge of the blatant misrepresentation for which they were held accountable.

The private information stores of several prestigious organizations, some of them very sensitive and personal in nature, have been lost, misplaced, or accessed by hackers – the details of the events becoming fodder for an indignant news media.

Corporate America, already under varying degrees of competitive and performance pressure, is now faced with compliance legislation and disclosure requirements that seek to right some of the wrongs done to consumers, investors, and employees alike. What follows is an analysis of the major pieces of process and data management compliance legislation, with a specific focus on the critical role that data availability plays in all of them. Access and process controls, internal and third party audits, reporting requirements and penalties for non-compliance are just a few of the areas that will be addressed on a per-measure basis.

#### **Healthcare Insurance Portability and Accountability Act of 1996 – (HIPAA)**

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services to establish national standards for electronic health care transactions and national

identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data, otherwise known as protected health information (PHI).

The Act was passed in August of 1996, with the original document calling for the Department of Health and Human Services to adopt standards for certain types of healthcare transactions, such as claims processing and billing, within 18 months of that date. Health plans were expected to adopt these same standards as practice within 24 months of their adoption by HHS, effectively opening a three and a half year window for analysis and adoption. Today, approaching a decade after the enactment of HIPAA into law, full uptake and adoption projections extend out until 2007, with future extensions of various types highly probable.

HIPAA applies to organizations called covered entities. Covered entities include all health plans, all healthcare clearinghouses and all providers who transmit HIPAA covered transactions. In February of 2003, the Final Rule adopting HIPAA standards for the security of electronic health information was published in the Federal Register. Among many other items, the standards called for appropriate measures to back up and store healthcare-related computer data files. Above the protestations of some members of Congress, the document specifically addressed the need of covered healthcare entities to back up their critical data stores, citing that the methodology and requirements would differ from one to another. In fact, the final security rule contains language making the implementation of a data backup plan a required portion of compliance with the rule, positioning backup as part of a 'required contingency plan' which also calls for a formal disaster recovery plan and an emergency mode operation plan. Further, the committee also listed data backup as 'addressable' in the Physical Safeguards section of the rule<sup>1</sup>, meaning that the covered entity needs to adopt the implementation specification as written in the rule, adopt another equally secure standard or have a well documented reason (other than strictly the cost of implementation) why the addressable implementation specification will not be adopted.

It is clear that the intent of HIPAA, particularly the Administrative Safeguards and Technical Safeguards sections of the Final Security Rule, is to help insure that a covered entity's sensitive data stores are protected both technically and operationally from unauthorized access and usage, and to insure that they can be recovered in the event of the loss or destruction of host hardware or infrastructure.

The majority of HIPAA compliance activity manifests as sensible business practices - things like locked server room or datacenter doors, password protected databases, access and process control documentation, and formal plans for disaster recovery and business continuity.

It is important to note that many of the key measures extend not only to large health insurance companies, but to their business associates, participating physicians and clearinghouses as well. Also worth clarifying is that business associates are not covered directly by HIPAA regulations, but are covered by contract with the covered entities that they provide products and/or services for. Like it or not, HIPAA has helped to create healthier and more secure physician business processes. In the past, physicians were content and within guidelines to back up to tape drives located within their offices. The new HIPAA security standards, which officially took effect April of 2005, mandate that the physician be able to access the data in case of an emergency so that operations can continue. The same holds true for health plans and clearinghouses.

Ideally, physicians, other covered entities and their business associates should back up their data to an offsite and secure facility, so that perils to the physical office and hardware would not substantially affect their ability to quickly resume business with an accurate and secure data set. In a recent article in a prominent international medical journal, a leading provider of financial and technical services to smaller physician's offices listed the lack of a data backup plan as one of three key areas of non-compliance by these entities<sup>2</sup>.

What are the costs of non-compliance? Let's disregard for a moment the clear and serious business implications for any entity that is publicly accused or exposed as having mishandled sensitive patient data. Instead we'll concentrate on the stated fines and imprisonment sanctions that are spelled out for us within the Act itself. Per section 1177, fines for any covered entity that knowingly uses, obtains, or discloses personally identifiable health information to another person range from \$50,000 to \$250,000 per case, depending on the nature and circumstances surrounding the offense. Violators can also face jail time ranging from one to ten years in addition to the fines<sup>3</sup>.

The message is clear. The sensitive and personal nature of the information required to do business in the healthcare sector also requires extraordinary measures to prevent it from being leaked or unintentionally shared with others during day-to-day operations. As of April 2005, more than 175 cases of alleged privacy violations had been referred to the Department of Justice (DOJ) for potential criminal prosecution.<sup>4</sup> While that number represents a small fraction of the nearly 11,000 complaints made during that same time period, recent entries in medical association journals indicate that investigative activity is on the rise. It is a safe bet that regulators and investigators from DOJ, the Office of Civil Rights and the Center for Medicaid and Medicare Services will undoubtedly be less inclined to show leniency as time goes by.

### **Data Backup Software and Services – Access controlled Data Insurance**

To be clear, there is no single software product or information technology service that can make an organization fully compliant with any of this legislation. The respective laws are complex and far-reaching, and were designed to enforce a level of integrity in operations and corporate philosophy that cannot be pulled from a box or jewel case. Remote Backup Software, through its ability to maintain secure copies of critical, sensitive data in a protected location, and to have them available for quick restore for required reporting or disclosure, addresses several of the criteria of compliance with all of them.

As enforcement of these laws increases, so does the need to have your data, and that of your clients, properly secured. Are you a member of the 'circle of trust' as referenced in GLB? Are you a HIPAA 'covered entity' or a business partner of one? Can you guarantee availability of critical reporting data for your SOX clients? It is time for IT service companies and businesses of all types to get serious about data security – and remote backup of data is a crucial and cost-effective component in compliance, business continuity, and disaster recovery planning.

#### **Acknowledgements and Sources:**

<sup>1</sup>Federal Register, Health Insurance Reform – Security Standards, February 2003

<sup>2</sup>International Journal of Micrographics and Optical Technology, Physicians Lack Data Backup Plans and Access Controls, January 2005

<sup>3</sup>University of Miami Ethics Program, Violation Penalties (HIPAA), May 2005

<sup>4</sup>California Medical Association, HHS Publishes HIPAA Enforcement Plan, April 2005

Media Contact information:  
John Neibel, President & Founder  
[Mirrored Storage, Inc.](#)  
P. 214-550-0550

Copyright © 2009, 2010 & 2011, [Mirrored Storage, Inc.](#) Any reuse without the expressed written permission of [Mirrored Storage, Inc.](#) is prohibited.

