Data Backup and Compliance Legislation: Three Reasons to get it Right

White Paper presented by:

REMOTE BACKUP SYSTEMS, INC.
ONLINE BACKUP SOFTWARE
http://remote-backup.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 three 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[1], 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[2].

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[3].

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.[4] 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.

The Financial Modernization Act of 1999 - Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB, includes provisions to protect consumers' personal financial information held by financial institutions. There are two principal parts to the privacy requirements as they relate to data management: the Financial Privacy Rule and the Safeguards Rule.

The GLB Act gives authority to eight federal agencies and the States to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These regulations apply to "financial institutions," which include not only banks, securities firms, and insurance

companies, but also companies providing many other types of non-traditional financial products and services to consumers. Among these services are those in the business of lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, residential real estate settlement services, collecting consumer debts, providing health insurance and an array of other activities. Such non-traditional financial institutions are also regulated by the FTC[5].

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information. The Financial Privacy rule requires covered institutions to spell out, in the form of a privacy notice, their information sharing practices. Most of us have seen these notices included with correspondence related to loan applications, account servicing, or credit card statements. Using a process detailed in the institutional privacy notices, consumers have the right to limit some – but not all – sharing of their information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The rule applies not only to financial institutions that collect information from their own customers, but also to businesses – such as credit reporting agencies – that receive customer information from those institutions. It is within the Safeguards section of GLB that the parameters for data safety at these institutions are clarified, and it is here also that the deficiencies of 'legacy' data protection methods are exposed. The section addresses distinct areas of safeguards which must be implemented, including Administrative, Technical, and Physical.

As in HIPAA regulations, many of the Administrative safeguards are designed to verify that reasonable steps are being taken to secure the sensitive data stores maintained by covered institutions. While most of these steps should be (and in many cases are already) taking place at the institutions, the Safeguards Rule mandates that the administrative steps be encapsulated in a written information security plan. The plan is required to include an assessment of risks and an evaluation of existing safeguards, the establishment of a comprehensive safeguards plan, contracting with vendors to facilitate the plan when appropriate, and regular testing and evaluation of the plan and practices as the covered entity's business scope or volume changes.

The Federal Trade Commission (FTC), which is a major oversight body for GLB, also indicates the need for employee education and training, information systems management, and managing system failures. These measures help to insure that data safeguards are robust and that all parties who come into contact with sensitive information are aware of company policies and the law.

The Information Systems component of GLB addresses the company's technological interfaces with client data, and can include analyses of network and software design, information processing, storage, transmission, retrieval, and disposal. Here again, The FTC strongly suggests several procedural and technological steps ranging from basic

security like locked file drawers and server rooms to backing up client data to a secure, encrypted and password-protected server.

Many of GLB's provisions are designed to ensure that basic steps are taken to ensure client data is only available to those employees who need it in the course of their work, and that it is securely off-limits to others. The Financial Privacy provisions were put in place to insure that the data is properly maintained and protected. The provisions related to information systems and managing systems failures help to insure that the institution maintains access to the data in order to resume operations after data loss, and to be able to provide documentation that would normally have been lost when and if the need or requirement arises.

As Federal agencies are empowered to enforce GLB under existing codes such as the Federal Deposit Insurance Act, penalties for non-compliance are substantial. Fines levied at guilty institutions can be up to $100,000 per violation at the national level and can also expose the covered institutions, especially those in the insurance sector, to state-level sanctions in many cases. In addition, the officers and directors of these companies can be held personally liable for civil penalties up to $10,000. For companies or individuals that employ 'pretexting' (the use of fraudulent or deceptive tactics to obtain private financial information) the monetary penalties can go even higher, and violators can face prison terms of 5 to 10 years in addition to the fines.

Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act, commonly referred to as 'SOX', was signed into law on July 30th 2002, and introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws"[6].

The legislation came about after a round of highly-publicized corporate scandals rocked the corporate world in the opening years of the new millennium; the most notable of these included the Enron collapse and subsequent revelations of accounting irregularities at WorldCom.

At the risk of oversimplifying a landmark piece of legislation, and speaking strictly as it relates to information technology, data backup, management processes and disclosures, the act contains several key sections.

Sections 103 and 104 are closely related, and provide details about the length of term (7 years) that accounting and auditing entities must retain all documents and data relating to audit reports of companies required to comply with SOX. While the physical paperwork can be maintained in various ways, electronic backup of digital records is highly advisable considering that investigators usually demand all versions of documents in their analysis. With encrypted, secure offsite backup of these files, they are protected from prying eyes or malicious intent, and virtually any version of a file can be retrieved very quickly for comparison, and for building the paper trail that proves that control processes were properly followed.

Section 105 addresses the confidential nature of the accounting and audit files prepared for and received by an organization's board of directors. Again, digital backup copies are the best bet for preserving these files because they can be encrypted and compressed prior to storage, and with the best remote backup solutions, remain encrypted and compressed in storage until they are restored to the original source location. This makes it virtually impossible for the contents of these sensitive documents to become known to, or to be 'restored' by anyone other than authorized individuals – clearly a critical piece of the compliance puzzle with regards to accounting and auditing firms.

Section 302 of the eleven-section law is entitled Corporate Responsibility for Financial Reports and is important because it places the responsibility of attesting to the content, accuracy, and (perhaps most importantly) the authenticity of financial reports issued by that organization squarely on the shoulders of executive management and the board of directors at public companies.

Section 404 also involves the placement of additional responsibility on senior management and corporate officers, but has implications that extend deep into the rank-and-file of the company as well. Initially, Section 404 seems to simply require an addendum to the company's annual report. This addendum, referred to as an internal control report, states that management is responsible for maintaining an "adequate internal control structure", and is also to include an assessment by management of the control structure's effectiveness[7].

The loss of data from any critical systems during the reporting processes can send the entire compliance scramble into a tailspin, and at the very least the corporate stewards will be required to log this deficiency in their periodic reports. In light of the contempt with which Congress has met previous corporate cover-up activity, the permanent loss of potentially revealing data in this manner could well be seen as a federal-level 'dog ate my homework' plea. Unfortunately, the media can act as a catalyst for speculation, spinning what might truly be an unfortunate event into a story that sends investors scrambling.

The bottom line? Compliance with Sarbanes Oxley depends heavily on reports created from sensitive data, without even the appearance of impropriety in its compilation. These reports must be generated from actual, factual data, with strict access and process safeguards all along the way and executive-authorized documentation to attest to the existence of and adherence to these safeguards. Remotely backing up the data that is crucial to the creation of these reports insures that localized hazards such as fire, theft, or opportunistic or vindictive employees are neutralized and that the mission-critical reports can be drawn from original data.

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:

[1]Federal Register, *Health Insurance Reform – Security Standards*, February 2003

[2] International Journal of Micrographics and Optical Technology, *Physicians Lack Data Backup Plans and Access Controls*, January 2005

[3] University of Miami Ethics Program, *Violation Penalties (HIPAA)*, May 2005

[4] California Medical Association, *HHS Publishes HIPAA Enforcement Plan*, April 2005

[5]Federal Trade Commission, *Financial Privacy: The Gramm-Leach Bliley Act*, online at ftc.gov

[6]Sarbanes Oxley Act Forum, *posting*, online at sarbanes-oxley-forum.com

[7]American Institute of Certified Public Accountants, *Summary of Sarbanes-Oxley Act of 2002* (Interpretation), online at aicpa.org

[8]Chris Apgar, Apgar and Associates – Special thanks for providing professional assistance and consultation

Media Contact information:

Tommy Gardner, Director of Sales and Marketing

Remote Backup Systems, Inc.

P. 901.850.9920 http://remote-backup.com