



## ***How DataSafe™ Helps Companies Meet Compliance Requirements***

*Published: February, 2007*

---

### **Abstract**

Companies, regardless of size, find themselves faced with data protection and retention regulations including state privacy laws, Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI), and the Gramm-Leach-Bliley Act. These regulations are changing the way companies retain and manage their records and data retention policies and plans are absolutely essential to meeting these regulatory requirements.

Failure to produce all relevant documents in an audit or court proceeding can lead to loss of the public trust and punitive actions including fines and imprisonment.

NetStandard's DataSafe™ product can help your company meet the data protection requirements dictated by these regulations.

---

**Contents**

Introduction .....	3
The Sarbanes-Oxley (SOX) Act of 2002.....	3
How DataSafe Helps Achieve SOX Compliance .....	3
Health Industry Portability and Accountability Act (HIPAA).....	4
How DataSafe Helps Achieve HIPAA Compliance .....	4
Payment Card Industry Data Security Standards (PCI) .....	6
How DataSafe Helps Achieve PCI Compliance .....	6
The Gramm-Leach-Bliley Act .....	7
Financial Privacy Rule.....	8
Safeguards Rule .....	8
Pretexting Protection .....	8
Definition of Financial Institutions .....	9
GLBA Enforcement .....	9
How DataSafe Helps Achieve GLBA Compliance .....	9

## Introduction

DataSafe provides encrypted online backup, recovery, and message level email back-up and restoration that can help your company achieve compliance with regulatory requirements including state privacy laws, Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act.

## The Sarbanes-Oxley (SOX) Act of 2002

The Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox; July 30, 2002) is a United States federal law passed in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Peregrine Systems and WorldCom (recently MCI and now currently part of Verizon Businesses). These scandals resulted in a decline of public trust in accounting and reporting practices. Named after sponsors Senator Paul Sarbanes (D-Md.) and Representative Michael G. Oxley (R-Oh.), the Act was approved by the House by a vote of 423-3 and by the Senate 99-0. The legislation is wide ranging and establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.<sup>1</sup>

### *How DataSafe Helps Achieve SOX Compliance*

Requirement	Regulatory Reference	NetStandard Solution
Record Retention	Section 103(a)(2)(A)(i) Prepare and maintain, for a period of not less than 7 years, audit work papers and other information related to any audit report, in sufficient detail to support the conclusions reached in such report;	DataSafe stores all identified data offsite in the NetStandard data center. Data can be retained for as long as the client needs.
Production of Records	Section 105(b)(2)(B) Requires the production of audit work papers and any other document or information in the possession of a registered public accounting firm or any associated person thereof, wherever domiciled, that the Board considers relevant or material to the investigation, and may inspect the books and records of such firm or associated person to verify the accuracy of any documents or information supplied;	DataSafe keeps multiple encrypted versions of important files. Data can be retained online and recovered whenever needed even if it is years later.
Retention of Complaints	Section 301(4)(A) The receipt, retention, and	DataSafe keeps all records safely stored in an encrypted

<sup>1</sup> Wikipedia, <http://en.wikipedia.org/wiki/Sarbanes-Oxley/>

Requirement	Regulatory Reference	NetStandard Solution
	treatment of complaints received -by the issuer regarding accounting, internal accounting controls, or auditing matters;	state at NSI's high availability data center including e-mails and images of documents that may have been scanned.
Internal Controls	Section 404(a)(1) States the responsibility of management to establish and maintain an adequate internal control structure and procedures for financial reporting	DataSafe keeps all records safely stored in an encrypted state at NSI's high availability data center. In the event of a disaster or accidental erasure or corruption of a database, your company's financial information will remain safe in the DataSafe.
Destruction or Alteration of Data	Section 802(a) Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.	DataSafe keeps multiple encrypted versions of important files and data can be retained online as long as required

## Health Industry Portability and Accountability Act (HIPAA)

The **Health Insurance Portability and Accountability Act (HIPAA)** was enacted by the [U.S. Congress](#) in [1996](#).

According to the [Centers for Medicare and Medicaid Services'](#) (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, [health insurance](#) plans, and employers.

The AS provisions also address the security and privacy of health data. <sup>2</sup>

### ***How DataSafe Helps Achieve HIPAA Compliance***

DataSafe can help your company fulfill the requirements of the Health Information Portability & Accountability Act (HIPAA), including data integrity, authentication, contingency planning, access and audit controls as they relate to electronically protected health information.

<sup>2</sup> Wikipedia, <http://en.wikipedia.org/wiki/HIPAA>

<b>Requirement</b>	<b>Regulatory Reference</b>	<b>NetStandard Solution</b>
Contingency Planning	<p>164.308(a)(7)(i) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.</p> <p>164.308(a)(7)(ii) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.</p>	DataSafe ensures that your data is encrypted and safely stored in NetStandard's high availability data center. In the event of a calamity, data can be quickly restored either at the customer site OR at a DR center of your choice. If needed, the data can be copied to a physical drive and physically transported to a designated site. Regardless of the method used, the data remains encrypted throughout the restoration process.
Access Controls	<p>164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).</p>	DataSafe authentication using a user name and password, strong encryption and non-escrowed keys provide assurance that unauthorized persons or software cannot access DataSafe data.
Audit Controls	<p>164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</p>	DataSafe automatically records an audit trail of all backups and restores. Detailed log reports can be generated for clients as they are required.
Data Integrity	<p>164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.</p> <p>164.312(c)(2) Mechanism to authenticate electronic protected health information (Addressable).</p>	DataSafe executes a 3-level Circular Redundancy Check (CRC) to ensure that data sent from the client is the data received and written to the Safe. Once data is backed up, it cannot be overwritten by accident OR removed.

Requirement	Regulatory Reference	NetStandard Solution
	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	
Authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	DataSafe restricts user access using a unique customer user name and password and the data is encrypted using a key known only to the customer.

## Payment Card Industry Data Security Standards (PCI)

The [Payment Card Industry Security Standards Council](#) was organized by the major credit card companies to provide world-wide open standards for data security and account protection. All of the major credit card and payment providers have adopted the data security standards of this organization. These standards are referred to as PCI data security standards. Companies who accept credit cards must adhere to these security standards.<sup>3</sup>

### ***How DataSafe Helps Achieve PCI Compliance***

DataSafe can help your company achieve PCI compliance. The payment card industry compliance and validation regulations apply to financial institutions, Internet vendors and retail merchants. The rules spell out what security measures must be taken to protect the private information of employers and employees during any transaction occurring with the use of a payment card. They also require certain auditing procedures. The Payment Card Industry Data Security Standard is used by all card brands to assure the security of the data gathered while an employee is making a transaction at a bank or participating vendor.

Requirement	Regulatory Reference	NetStandard Solution
<b>Build and Maintain a Secure Network</b>	<i>Requirement 1:</i> Install and maintain a firewall configuration to protect cardholder data <i>Requirement 2:</i> Do not use vendor-supplied defaults for system passwords and other security parameters	DataSafe works through the customer's firewall. Customers allow traffic to/from NetStandard using predefined ports. DataSafe encrypts all data before, during and after transmission using a non-escrowed encryption key owned by the transmitting customer.  DataSafe authentication using a user name and password, strong encryption and non-escrowed keys provide assurance that unauthorized persons or software cannot access DataSafe data.
<b>Protect Cardholder Data</b>	<i>Requirement 3:</i> Protect stored cardholder data	DataSafe encrypts all data before, during and after

<sup>3</sup> <http://www.pcisecuritystandards.org/>

Requirement	Regulatory Reference	NetStandard Solution
	<p><i>Requirement 4:</i> Encrypt transmission of cardholder data across open, public networks</p> <p><i>Requirement 6:</i> Develop and maintain secure systems and applications</p>	<p>transmission using a non-escrowed encryption key owned by the transmitting customer.</p> <p>DataSafe requires authentication using a user name and password, strong encryption and non-escrowed keys provide assurance that unauthorized persons or software cannot access DataSafe data.</p>
<p><b>Implement Strong Access Control Measures</b></p>	<p><i>Requirement 7:</i> Restrict access to cardholder data by business need-to-know</p> <p><i>Requirement 8:</i> Assign a unique ID to each person with computer access</p> <p><i>Requirement 9:</i> Restrict physical access to cardholder data</p>	<p>DataSafe encrypts all data before, during and after transmission using a non-escrowed encryption key owned by the transmitting customer.</p> <p>DataSafe requires authentication using a user name and password, strong encryption and non-escrowed keys provide assurance that unauthorized persons or software cannot access DataSafe data.</p>

## The Gramm-Leach-Bliley Act

The **Gramm-Leach-Bliley Act**, also known as the Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (November 12, 1999), is an Act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies and insurance companies. The Gramm-Leach-Bliley Act (GLBA) allowed commercial and investment banks to consolidate. In terms of compliance, the key rules under the Act include:

- *The Financial Privacy Rule* which governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information.
- *The Safeguards Rule* requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions.<sup>4</sup>

<sup>4</sup> [http://en.wikipedia.org/wiki/Gramm-Leach-Bliley\\_Act](http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act)

## ***Financial Privacy Rule***

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 [U.S.C. § 6801](#) through 15 [U.S.C. § 6809](#))

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt-out of the information being shared with unaffiliated parties per the [Fair Credit Reporting Act](#). Should the privacy policy change at any point in time, the consumer must be notified again for acceptance. Each time the privacy notice is reestablished, the consumer has the right to opt-out again. The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement. In summary, the financial privacy rule provides for a privacy policy agreement between the company and the consumer pertaining to the protection of the consumer's personal nonpublic information.

## ***Safeguards Rule***

(Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 [U.S.C. § 6801](#) through 15 [U.S.C. § 6809](#))

The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. (The Safeguards Rule also applies to information of those no longer consumers of the financial institution.) This plan must include:

- Denoting at least one employee to manage the safeguards,
- Constructing a thorough [risk management] on each department handling the nonpublic information,
- Develop, monitor, and test a program to secure the information, and
- Change the safeguards as needed with the changes in how information is collected, stored, and used.

The Safeguards Rule forces financial institutions to take a closer look at how they manage private data and to do a risk analysis on their current processes. No process is perfect, so this has meant that every financial institution has had to make some effort to comply with the GLBA.

## ***Pretexting Protection***

(Subtitle B: Fraudulent Access to Financial Information, codified at 15 [U.S.C. § 6821](#) through 15 [U.S.C. § 6827](#))

[Pretexting](#) (sometimes referred to as "social engineering") occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (i.e., using a "phony" website or email to collect data). The GLBA has provisions that require the financial institution to take all precautions necessary to protect and

defend the consumer and associated nonpublic information. Pretexting is illegal and punishable by law beyond any recognition by the GLBA.

## ***Definition of Financial Institutions***

The GLBA defines “financial institutions” as: ...”companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission (FTC) has jurisdiction over financial institutions similar to, and including, these:

- non-bank mortgage lenders,
- loan brokers,
- some financial or investment advisers,
- debt collectors,
- tax return preparers,
- banks, and
- real estate settlement service providers.

These companies must also be considered significantly engaged in the financial service or production that defines them as a “financial institution”.

Insurance has jurisdiction first by the state, provided the state law at minimum complies with the GLBA. State law can require greater compliance, but not less than what is otherwise required by the GLBA.

## ***GLBA Enforcement***

Violation of the *GLBA* may result in a civil action brought by the [United States Attorney General](#). The penalties, as amended under the [Financial Institution Privacy Protection Act](#) of 2003 (108th CONGRESS - 1st Session - S. 1458; To amend the *Gramm-Leach-Bliley Act* to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes., In The Senate of the United States, July 25 (legislative day, JULY 21), 2003)include,

- “the financial institution shall be subject to a civil penalty of not more than \$100,000 for each such violation”
- “the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation”.

## ***How DataSafe Helps Achieve GLBA Compliance***

<b>Requirement</b>	<b>Regulatory Reference</b>	<b>NetStandard Solution</b>
<b>SafeGuards Rule</b>	<ul style="list-style-type: none"> <li>• Denoting at least one employee to manage the safeguards,</li> <li>• Constructing a thorough [risk management] on each department handling the nonpublic information,</li> <li>• Develop, monitor, and test a program to secure the information, and</li> <li>• Change the safeguards as needed with the changes in</li> </ul>	<ul style="list-style-type: none"> <li>• DataSafe encrypts all data before, during and after transmission using a non-escrowed encryption key owned by the transmitting customer. Customers can designate one employee to manage the safety of that key.</li> <li>• DataSafe facilitates back-up set creation that allows customers to ensure data</li> </ul>

<b>Requirement</b>	<b>Regulatory Reference</b>	<b>NetStandard Solution</b>
	how information is collected, stored, and used.	is encrypted, stored and recoverable at an offsite location. <ul style="list-style-type: none"><li>• DataSafe facilitates message level back-ups of e-mail.</li></ul>