

# A Guide to Email Regulatory Compliance

**Kevin Prince**  
Chief Technology Officer  
Perimeter eSecurity



7900 E. UNION AVE, SUITE 800, DENVER CO 80237  
PHONE - 800.653.0179  
INFO@CORPX.USA.NET  
WWW.USA.NET

## THE USE OF EMAIL

Email has become the standard for basic communications worldwide. While IM, SMS, mobile phones, Twitter, and many other communication methods exist and are popular, nothing rivals the ubiquity and diversity of email. Email is not just a way to send a message to someone anywhere in the world in a matter of moments, but acts as our personal filing cabinet for document management and communication storage, our calendar, mobile device synchronization, contact list manager, and our daily prioritized task manager.

Furthermore, many individuals have multiple email addresses, such as business and personal email. Sometimes our mail is stored remotely, sometimes locally on our individual computers, and often both.

Due to the early adoption of email (prior to so many of the advances in email security technology), there are many gaps and methods of exploit. While email is commonly used to transport private or sensitive information, these security holes often lead to data exploit, fraud, and identity theft. As a result many laws have been passed to more adequately secure private and sensitive information, many of them specifically requiring better email security.

## THE REGULATORY LANDSCAPE

If you want to start a business that isn't bound by any data security and privacy laws or regulations, you will have a tough time. It would mean you don't capture customer information, don't accept many forms of payments (including credit cards), you aren't a public company, you won't do business with the government. In fact, on top of the federal government, almost all US states have privacy laws that would prevent you from performing business.

REGULATION	WHAT IS IT?	IMPACTED ORGANIZATIONS
GLBA	The Gramm-Leach-Bliley Act (commonly called GLB or GLBA) is also known as the Financial Modernization Act of 1999. The GLB Act includes provisions to protect all consumers' personal financial information held by financial institutions.	The GLB Act applies to "financial institutions" - businesses that offer financial products or services. Financial institutions include banks, insurance companies, and securities firms. Also, non-traditional financial institutions include, but are not limited to, state-registered investment advisors, auto dealers engaged in leasing and financing, professional tax preparers, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies, retailers that issue credit cards to consumers, check-cashing businesses, consumer debt-collecting firms, and payday lenders.
FRCPP	The Federal Rules of Civil Procedure apply to any organization that has the potential to be involved in litigation in the U.S. Federal Court system. The amendments, which went into effect on December 1, 2006, mandate that companies be prepared for electronic discovery. The organization must know where their data is, how to retrieve it, how to meet data requests and they must determine what data will not be subject to search.	Any organization in any industry that has the potential of being involved in litigation in the U.S. Federal Court system. There are not many business types that are not subject to FRCPP. This includes any international business that does business in the U.S.

REGULATION	WHAT IS IT?	IMPACTED ORGANIZATIONS
SOX	The Sarbanes-Oxley Act, commonly called SOX, sets forth records management and retention policies for all public companies. SOX was enacted in 2002 in response to corporate scandals involving large, public corporations.	All companies under the jurisdiction of the U.S. Securities and Exchange Commission must comply with the Sarbanes-Oxley Act. Basically, any publicly-traded company must follow Sarbanes-Oxley regulations.
HIPAA	HIPAA stands for the Health Insurance Portability and Accountability Act. HIPAA calls for national standards for electronic healthcare transactions, among other requirements. HIPAA requires that organizations that deal with electronic patient healthcare information protect the security and confidentiality of that data.	Virtually all organizations that deal with electronic patient healthcare information are affected. This includes (but is not limited to): healthcare providers, health plans, physicians' offices, public health authorities, healthcare clearinghouses, pharmacies, organ, blood and sperm donation banks, and long-term care facilities. Also included are those entities that handle, exchange or store private electronic health information, such as self-insured employers, life insurers, billing agencies, information systems vendors, various service organizations, and universities. In many cases, HIPAA provisions have led to extensive changes with regard to medical record keeping and billing systems.
Data Breach Notification Laws	There are about 46 states that now have data breach notification laws. See <a href="http://www.atthebreach.com/security/states-with-data-breach-notification-laws/">http://www.atthebreach.com/security/states-with-data-breach-notification-laws/</a>	All companies that reside within the 46 states that currently have data breach notification laws. This includes companies that have customers, employees, or facilities in any of the 46 states with data breach notification laws.
NRS 597.970	Nevada's Electronic Transmission Encryption Law Nevada is the nation's first data encryption law, which prohibits businesses from electronically transferring customers' personal data outside their organization unless it is encrypted.	All organizations that reside within Nevada and those that communicate electronically with those organizations.
201 CMR 17.00	Massachusetts has passed a similar law to Nevada's but most of it doesn't go into effect until 1/1/2010. The law requires companies to implement a comprehensive data security plan that includes encryption.	All organizations that reside within Massachusetts and those that communicate electronically with those organizations.
FERPA	The Family Educational Rights and Privacy Act governs the privacy of student records in any medium, including email.	Any institution that accepts money from the Department of Education.
SEC Rule 17a-4	The SEC ruled that brokerage houses must, under penalty of law, control all electronic communications. Rule 17a-4(f) defines the strict SEC requirements for storage of these electronic records.	Firms conducting business in security futures products.
PCI-DSS	The Payment Card Industry Data Security Standard is a set of requirements that merchants who accept credit cards must comply with.	Organizations that accept credit cards for payment transactions.

The reality is that most companies have to adhere to several laws and regulations. All these various regulations essentially want to accomplish the same thing - protect private or sensitive information. Many security frameworks and best practices use a C.I.A. approach: Confidentiality, Integrity, and Availability. Confidentiality means keeping the data private so only authorized individuals can access and use it. Integrity is the process by which only authorized individuals can modify, update, or change the data. Availability means that the data is available for authorized business use whenever it is needed. C.I.A. is a best practices approach to information security, that if done correctly, will satisfy nearly every regulation you are required to meet.

## **POLICIES & PROCEDURES**

Policy and procedural documents need to be created around the email life cycle. The email life cycle includes message:

- Creation
- Transport (Data In Motion)
- Management
- Archival (Data At Rest)
- Disposal
- Business Continuity

Regulations exist pertaining to each aspect of the email life cycle, specifically when the contents contain sensitive or private information. Policies and procedures that address the email life cycle will include:

- What is defined as sensitive or private information
- Where sensitive data is stored
- Who is authorized to access sensitive data (send, receive, management, archival access, etc.)
- When and how individuals are authorized to access and use the data
- Taking into account both internal communications and external communications
- How long the data is stored
- Upon what basis can the data be deleted

Policies and procedures will be tailored to a specific company's use of the data, their business processes, etc. As such, the specific elements within the policies and procedures will vary from organization to organization.

## **RISK ANALYSIS**

The second step once policies and procedures are written is to do a risk analysis. You want to map policies and procedures to existing business processes and risk mitigation solutions in an effort to identify security and procedural gaps that puts your sensitive data at risk. You then prioritize these gaps from the most severe to the least severe. It is entirely likely that you will choose or not be able to address

all of the issues. Some issues you will never address, and others will be dealt with at a later date.

With your prioritized list in front of you, you can draw two lines effectively separating the list into three sections. The top section are things you are going to address now. The second section are things that need to be addressed, but can be addressed later, often in the next budget cycle. The third section are those things that you are choosing not to address. They are usually less severe or perhaps things that are difficult to improve; but can also simply be things that the return on investment (ROI) is simply not there. These items you will assume as a business risk and not spend time or resources on improving. Now you can select the solutions that are best suited to address the specific gaps identified by your risk analysis.

## AUDITING AND REPORTING

Once policies and procedures have been put into place, a risk assessment has occurred, and a gap analysis performed organizations can begin to utilize various solutions (both technology based and non-technical) to audit and report on the confidentiality, integrity, and availability of sensitive data. There are several ways of approaching the auditing and enforcement of sensitive data.



“Compliance” does not equal “Secure”. There are some companies that want to spend the least in terms of time and resources to be compliant with regulations. This approach by itself allows companies to get check marks for compliance, but are not necessarily addressing all or their most critical data security needs. There are many examples (especially under the Payment Card Industry Data Security Standard, a.k.a. PCI-DSS) where a company received PCI certification, but then experienced a data breach.

Regulations are designed to be minimum standards that must apply to large numbers of very different organizations. They should be looked at as required guidelines for where their security posture should begin, but not end. However, there are many organizations that only have the time or resources to achieve this level of security. If so, the following chart may help you identify the various technologies available to help you achieve regulatory compliance.

REGULATION	POLICIES & PROCEDURES	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	AUDITING & REPORTING
GLBA	Content Filtering	Encrypted Email	Encrypted Email, AV, SPAM Filtering	Archiving, Email Hosting, AV	Compliance Review, Compliance Reporting
FRCP			Archiving	Archiving	Compliance Review, Compliance Reporting
SOX	Content Filtering		Archiving	Archiving	Compliance Reporting
HIPAA	Content Filtering	Encrypted Email	Encrypted Email, AV, SPAM Filtering	AV	Compliance Reporting
NRS 597.970	Content Filtering	Encrypted Email			Compliance Reporting
201 CMR 17.00	Content Filtering	Encrypted Email			Compliance Reporting
FERPA	Content Filtering	Encrypted Email			Compliance Reporting
SEC Rule 17a-4	Content Filtering, Archiving		Archiving	Archiving	Compliance Review, Compliance Reporting
PCI-DSS	Content Filtering	Encrypted Email	AV, SPAM Filtering	AV	Compliance Reporting

## THE TECHNOLOGY APPROACH

Once a risk analysis is done, some organizations are immediately aware of the gaps in their security program and want to implement solutions to mitigate those risks. However, they want to get the greatest coverage from a regulatory as well as best practices perspective. The following chart is designed to map email technologies to regulation and best practices.

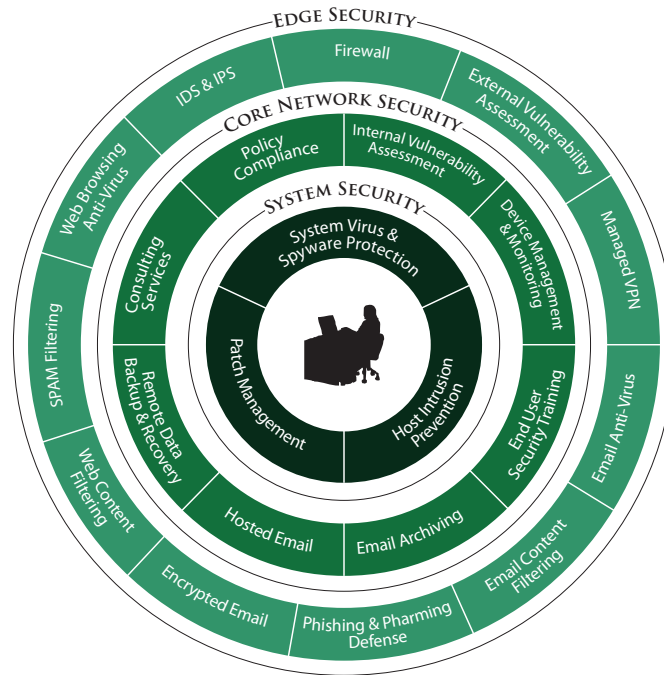
SERVICE	REGULATION(S)	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
EMAIL HOSTING		X	X	X
ANTI-VIRUS	GLBA, HIPAA, PCI		X	X
SPAM Filtering	GLBA, HIPAA, PCI		X	X
Encrypted Email	GLBA, HIPAA, NRS 597.970, 201 CRM 17.00, FERPA, PCI	X		
Archiving	GLBA, FRCP, SOX, SEC Rule 17a-4		X	X
Content Filtering	GLBA, SOX, HIPAA, NRS 597.970, 201 CRM 17.00, FERPA, PCI, SEC Rule 17a-4	X		
Compliance Review	GLBA, FRCP, SEC Rule 17a-4	X		

## THE LAYERED SECURITY APPROACH

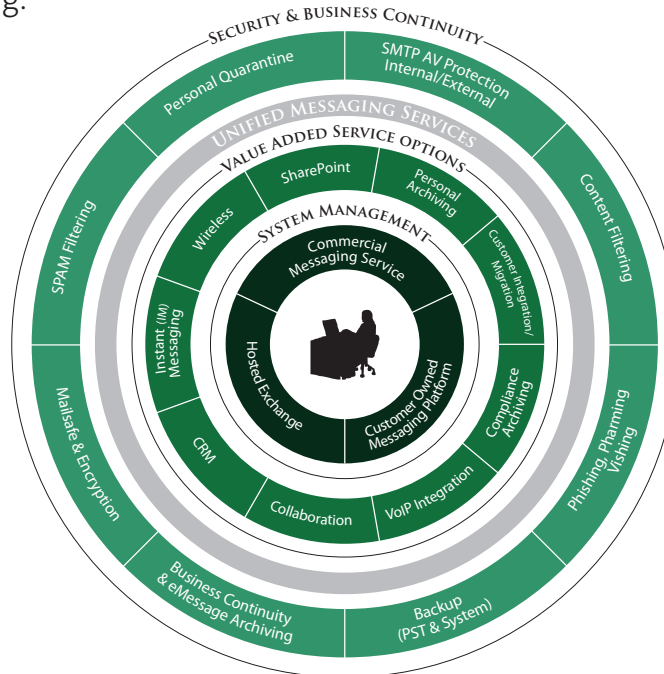
Another approach which requires an organization to take a step back from email specifically is the layered security approach. Organizations that have a desire to follow best practices or comply with regulations usually have more areas to address than just email. As such, a more holistic approach is needed to assume a comprehensive network security program for overall compliance and best practices. For example, one might overlook that the email system itself needs to be protected with various technologies such as firewalls, intrusion detection systems, and so forth. So while email is a critical element of modern day business, it is only one aspect of compliance and best practices.

Security professionals agree that there is no silver bullet to security or compliance. A multi layer approach should be taken to address all aspects of an organizations regulatory needs as well as best practices for data security. Edge security is meant to protect your organization primarily from Internet-based threats. Core network security is what protects elements of the inside of your network from 3rd parties, contractors, other insiders, remote offices, etc. System security are solutions that you load directly on an asset (server, workstation, laptop) that you want to protect (See diagram on next page).

A layered security approach takes into account many solutions beyond what is needed for an email environment. This comprehensive approach offers organizations the opportunity to fulfill their regulatory and best security practice needs.



A layered approach can be applied to email individually if best practices (which encompass regulatory compliance) is to be achieved. This is especially true when an email platform is used for messaging, mobile devices, calendaring, document management, and more. An email layered security diagram might look like the following:



Each organization has to review their own needs, resources, state of security, and goals to select the approach that works best for them.

## **SOLUTION SUMMARY**

Once the approach has been selected and the work has been done, organizations often want to know more about the specific solutions that will address their needs. This solution summary is designed to be a first step in the evaluation of specific services that can address security best practice and regulatory compliance.

### **MICROSOFT HOSTED EXCHANGE SERVICES**

Our customers enjoy all the benefits and features of an enterprise-class system without the risks of managing an on-premise solution. USA.NET messaging experts manage the hardware, software, upgrade/patch management of email and the adjacent services in our four fully-redundant data centers. Our operations are managed using a multi-layer security model that cover every aspect of the people, process and technology associated with delivering a reliable, secure and compliant email including:

- Gated, guarded and 24/7 monitored facilities with need-only access
- Employee background checks and on-going training/certification
- Multi-layer security at all operation levels including a strong perimeter defense with encryption, anti-virus, anti-spam protections
- Full daily backups of data stored in off-site locations
- Tightly integrated compliance tools such as archiving, encryption and content filtering
- 24x7x365 manned operations by fully certified engineers
- Sas70 Type-II audited

In addition to the compliance benefits, USA.NET also delivers the benefits of a hosted solution, which includes:

- Eliminating the need for large CAPEX on infrastructure
- Low and Predictable on-going costs
- Advanced features such as secure wireless, mobile data synchronization including calendars, contacts and notes
- On-demand services that give flexibility to scale up and scale down as needed based on per user/per month pricing
- 24/7 support

Our solution includes a Web-based administration tool that gives you control of your users, storage and service selection. Your email will be fast, reliable and secure, allowing you to focus on your core business instead of the email infrastructure needed to support it.

### **MESSAGING COMPLIANCE MANAGER**

USA.NET provides a quick, easy and economical email, IM and email archiving system that meets the rigid mandates of the SEC, FINRA, HIPAA, SOX, and the Federal Rules for Civil Procedures

(FRCP). Standard email archiving solutions don't satisfy the regulatory, discovery, and retention requirements for electronic records, which means an automated email archiving solution is necessary. Our solution safely stores your messages off-site and makes it easy to fulfill e-discovery and audit requests. Designed for today's needs and architected for tomorrow's changing regulatory environment, our email archiving solution will always meet your compliance needs.

## **MESSAGING CONTINUITY & ARCHIVING**

USA.NET has developed an email archiving system that securely stores all incoming and outgoing email while providing each user access to his/her archive through a web-based portal. Our Messaging Continuity & Archiving solution safely stores your messages off-site in our secure data center and makes it easy to fulfill e-discovery and audit requests while maintaining business continuity.

Our solution includes an archive portal that allows end users to access their own archives. We host the archive, thus relieving hardware on the customer's network from storage and access duties. Roles are created and assigned directly in the portal. Supervisory accounts are one role that can be set up and provide access to other employees' archives. The portal also allows for the creation of user groups for easy maintenance.

All messages can be recovered back to the user's inbox with a single click. Also, all users have the ability to send and receive messages directly from the archive. The message interface contains many parallel elements to popular email programs, so users will be productive on day one without portal training.

## **EMAIL ANTI-VIRUS**

New email viruses are released daily, any one of which can spread throughout your organization within a matter of minutes. Unfortunately, most anti-virus programs are ineffective at fighting new email viruses because of the time required to research, locate, download and deploy the latest virus definitions.

In the event of a new virus outbreak, the most critical and vulnerable time for any organization is the 4-8 hour window of time between the outbreak and the time that new signature files are available. USA.NET's staff of security professionals writes temporary "custom real time" gateway filters to defend our customers' network during this dangerous time. Our Email Anti-Virus Filtering system blocks both inbound viruses before they enter your network as well as outbound viruses on their way to clients or partners.

## **SPAM FILTERING**

Since a growing population of sophisticated SPAMMERS continue to evade basic filtering and detection by using forged headers, disguised identities, and constantly changing message content, reactive solutions to SPAM have become obsolete. To combat this threat, USA.NET uses a proactive solution.

Our server-side SPAM fighting solution seeks out possible SPAM and stops it. This approach defuses attacks before they inconvenience your employees, present potential legal liability, overwhelm your networks, and escalate your costs. In addition, USA.NET's anti SPAM service protects against productivity loss and vulnerability of informational assets associated with unsolicited or malicious email.

## **EMAIL CONTENT FILTERING**

Email is often credited with revolutionizing business communication and enhancing productivity. Its simplicity, speed of transmission and low cost make it a powerful means of communicating with colleagues, customers and suppliers. The ease and speed at which email messages can be forwarded to many recipients can present a range of risks to organizations if not sufficiently controlled. These risks include: breach of confidentiality, damage to reputation, lost productivity, legal liability and more.

In order to protect against unauthorized email distribution of sensitive information, USA.NET has developed an Email Content Filtering service which gives your organization the ability to block messages based on specific words or phrases found in the message subject, message body, as well as any attachments. Messages can also be filtered based on character sets (i.e. language types). Any filtered messages are delivered to quarantine for administrative review.

## **MAILSAFE ENCRYPTED EMAIL**

Under GLBA, HIPAA, California Disclosure Law, FFIEC guidelines and other state and federal regulations, regulators and auditors are warning businesses against transmitting sensitive data in clear text over regular email. While most organizations have a formal email usage policy, the problem is that most organizations have no way to enforce it. MailSafe™ does just that while providing a mechanism to send confidential information via encrypted email at the same time. With MailSafe™, you can quickly and privately send statements, lending documents, patient records, trust documents, and other important information to your customers, law offices, and business partners.

USA.NET's MailSafe™ service provides an easy to use solution for sending electronic messages securely to anyone via the Internet. MailSafe™ is designed to ensure regulatory compliance while remaining as simple as possible for the user. There is no software to download and install, and there are no keys to manage and distribute.

The MailSafe™ system inspects all outbound email from your organization and automatically redirects messages that contain sensitive content through a secure, encrypted channel. This policy driven feature guarantees that all users comply with your security policies.

## APPENDIX

(individual regulations and their requirements impacting email)

### PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)

The PCI-DSS has 12 requirements that must be complied with by merchants. Requirement number 4 specifically calls out email compliance.

- 4: Encrypt transmission of cardholder data across open, public networks
- 4.1: Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?
  - Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, email, instant messaging, chat)?

### GRAMM-LEACH-BLILEY ACT (GLBA)

Today, the vast majority of organizations use email to communicate internally and as a vehicle for the exchange of documents and correspondence between businesses and consumers. Since personal financial information can be transmitted by and retained in electronic formats, it is critical to ensure that the management of such records complies with GLBA. The safeguards rule requires financial institutions to have reasonable policies and procedures to ensure the security and confidentiality of customer information (for both current and former customers). The plan must include denoting at least one employee to manage the safeguards, doing a risk analysis on current processes, developing and monitoring a program to secure the information, and making adjustments to the security plan as needed.

- Section **6801 (b)(1)**: Companies must ensure that email messages are kept secure and encrypted when being transmitted over a link.

### SEC RULE 17A-4

The SEC ruled that brokerage houses must, under penalty of law (specifically SEC 17a3/4, NASD 3010 and Sarbanes-Oxley Act 2002 “SOX”) control all electronic communications. Rule 17a-4(f) defines the strict SEC requirements for storage of these electronic records.

Many types of documents are governed by Rule 17a-4, including “all communication sent by such member, broker, or dealer (including inter-office memoranda and communications) relating to his business as such”, as well as agreements, statements, bills, and many other records.

A key aspect of the SEC Rule 17a-4 is that the digital storage system must preserve the records in a non-editable, non-rewritable and non-erasable format. Systems that attempt to use authentication, hashing, fingerprinting, or other method to prove that editable data has not been tampered with is not sufficient for compliance.

The Rule 17a-4(f)(ii) states the electronic storage media must:

- Preserve the records exclusively in a non-rewriteable, non-erasable format;
- Verify automatically the quality and accuracy of the storage media recording process;
- Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and
- Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.

## **FEDERAL RULES OF CIVIL PROCEDURE (FRCP)**

On December 1, 2006 new amendments to the FRCP went into effect. Rules 16, 26, 33, 34, 37 and 45 and revisions to Form 35 are aimed at electronically stored information (ESI). These are technical amendments regarding discovery of ESI to the scope of information that a person receiving the subpoena must search. Additionally, the subpoena may specify the form in which the ESI is to be produced.

## **SARBANES-OXLEY (SOX)**

Requires that each broker-dealer keep originals of all communications received and copies of all communications sent by the firm relating to its business as a broker-dealer as well as certain types of public communications. The Commission has stated that the content and audience of the email message determine whether a copy must be preserved.

- **Section 302: Corporate Responsibility for Financial Reports**  
This section requires that CFOs and CEOs personally certify and be accountable for their firms' financial records and accounting.
- **Section 103: Auditing, Quality Control and Independence Standard and Rules**  
Requires companies to "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."
- **Section 105: Investigations and Disciplinary Proceedings**  
Requires "the production of audit work papers and any other document or information in the possession of a registered public accounting firm or any 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.”

- **Section 404: Management Assessment of Internal Controls**

Requires companies to report on the effectiveness of internal controls regarding financial reporting. Since internal business decisions and data are discussed, transported and stored in corporate email systems, ensuring that data cannot be accessed or tampered with is critical to the reliability of financial reporting.

Under SOX, corporate email messages have achieved the same status as other commonly used business documents and are subject to the same rules.

## **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**

HIPAA is designed to help organizations maintain security of patient information.

- Mandates the security of electronic medical records pertaining to an individual, requiring that covered entities ensure the confidentiality, integrity, and availability of all electronic protected health information that the entity creates, receives, maintains, or transmits.
- Requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of all electronic protected health information, protect against reasonably anticipated uses or disclosures of such information, and ensure compliance by their workforce.

## **NEVADA DATA ENCRYPTION LAW (NRS 597.970)**

Nevada put into effect the nation’s first data encryption law. This law prohibits businesses from electronically transferring customers’ personal data outside their organization unless it is encrypted. Nevada defines “personal information” as a person’s first and last name combined with social security, driver’s license or bank account, credit or debit card numbers accompanied by a security code or password that allows an unauthorized user to have access to the account -- all of which now need to be encrypted when being transferred electronically.

## **MASSACHUSETTS DATA ENCRYPTION LAW (201 CMR 17.00)**

A new Massachusetts law scheduled to take effect in May has been extended to Jan. 1, 2010, giving businesses more time to address and deploy technologies that tighten control of consumer data.

The law requires any firm conducting business with state residents to deploy encryption and protect against data leakage. A combination of a person’s name along with their Social Security number,

bank account number or credit card number must be encrypted when stored on portable devices or transmitted wirelessly on public networks according to the new law.

Encryption of personal information on portable devices carrying identity data like laptops, PDAs and flash drives must also be completed by Jan. 1, 2010.

### **ABOUT THE AUTHOR**

Named Chief Technology Officer of Perimeter in 2009, Kevin Prince spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise.

With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk. Mr. Prince has trained federal examiners for several years.

### **ABOUT USA.NET**

Founded in 1996, USA.NET is the recognized leader in hosted messaging and collaboration. The company offers a wide range services that solve customer requirements regardless of size, geographic location or complexity of need. From its proprietary, Unix-based Commercial Messaging Service (CMS), to its Hosted Exchange platform, USA.NET services SOHOs to major enterprises world-wide through its ability to highly customize each customer's messaging solution. The company offers over 20 enhanced services including mobility, archiving, encryption, content filtering and a variety of security services. USA.NET is a Microsoft Gold Certified Partner with competencies in Hosting, Security, Mobility and Advanced Infrastructure Solutions. USA.NET manages over 1M mailboxes for thousands of business clients across 120 countries. USA.NET is a wholly owned subsidiary of Perimeter eSecurity. Visit our website at [www.usa.net](http://www.usa.net) for more information or call us at 800.653.0179. You Run Your Business, We'll Run Your Email™.

### **ABOUT PERIMETER eSECURITY**

Perimeter is the trusted market leader of information security services that delivers enterprise-class protection and compliance for businesses of any size. Through its cost-effective security-as-a-software platform, Perimeter offers the most comprehensive compliance, security and messaging services that include but aren't limited to: hosted email, encrypted email, firewall management and monitoring, vulnerability scanning, host intrusion and prevention, email antivirus and spam, remote data backup and email archiving.

As companies struggle with the increasing cost, complexity and stringent compliance requirements associated with their information intensive businesses, Perimeter is the only provider that can simultaneously reduce the cost, manage all of the complexity and meet all of the compliance requirements from a single platform.

Headquartered in Milford, CT, with seven geographically distributed technical operations centers and three redundant datacenters, Perimeter's on demand services, which are offered both on a Network (in-the-cloud) and CPE (customer-provided equipment) basis, are validated by TruSecure and guaranteed for current and future regulatory compliance. If you would like to speak with us or view a product demo, please don't hesitate to call at 800.234.2175 Option #2 or visit our web site at [www.PerimeterUSA.com](http://www.PerimeterUSA.com).