

Encryption Laws and Compliance for the U.S.A

There is no “OOPS” clause in privacy legislation

The Echoworx suite of products can help organizations reduce the challenges and complexity of regulatory compliance by allowing IT and Administrators total control of their email environment. It provides them with the tools needed to help them comply with industry regulations such as HIPAA, GLBA, SOX, and others.

These tools can help organizations identify compliance issues and manage their infrastructure. Once applied, they can re-direct, prevent distribution or encrypt confidential information based on pre-defined policies.

The Echoworx policy engine automatically enforces compliance. All encrypted messages are digitally signed and can be validated to prove compliance as and when required



3 steps to Compliance:

1. Develop privacy policies and

- a. Define policies
- b. Create clear rules for the distribution of confidential info
- c. Provide and support an easy to use technical solution to enforce policies and procedures

2. Eliminate human error

- a. People make mistakes
- b. Most data is compromised inadvertently
- c. Up to 80% of breaches are caused internally

3. Protect confidential information

- a. Apply encryption to all confidential info
- b. Enforce encryption automatically using policy-based encryption at the gateway

WWW.ECHOWORX.COM

HIPAA (Health Insurance Portability & Accountability Act)

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information. **HIPAA mandates that all protected health information (PHI) should be encrypted on public networks (S.164) and digitally signed (S.142).** February 2009 saw the introduction of HITECH legislation which instituted criminal penalties for HIPAA violations. These penalties include four levels of increased culpability and fines of up to \$1.5 million per incident. HIPAA/HITECH rules have been a primary driver in the adoption of email encryption technology.

Massachusetts Encryption Law

Massachusetts has established its own **encryption law**. The Massachusetts mandate (201 CMR17.00), enacted in September 2008 with a compliance deadline of March 1,2010, requires that any organization that owns, licenses, stores or maintains personal information about a resident of Massachusetts follows a set of information-security requirements. This standard includes all businesses—whether in Massachusetts or not—that store data about a resident of the state.

To comply with this law, businesses must control passwords so they are secure; **encrypt all personal information stored on laptops and other portable devices**; and maintain up-to-date firewall protection and security software to protect personal information. Penalties for noncompliance with the Massachusetts standard are a civil penalty of \$5,000 for each violation.

California Encryption Law

California Senate Bill 1386 became effective in 2003 which requires individuals, businesses and government organizations in the state to notify Californians if their personal information is disclosed during a security breach.

The bill defines personal information as an individual's name accompanied by their Social Security number, driver's license number, bank account number or credit or debit card number.

California bill, AB 1950, mandates that **all organizations that use personal electronic records establish precautionary measures to protect personal data**. Senate Bill 440 requires California agencies, individuals and organizations that contract with California to encrypt personal data on all state-owned portable computing and storage devices.

Michigan Encryption Law

In 2008, Michigan Senator Randy Richardville introduced legislation for a state encryption law.

The bill mandated **companies that collect personal identifying information to store that information in a computerized database in an encrypted format**. According to the proposed bill, companies that violate the statute could be subjected to a fine, imprisonment or civil action.

The proposed Michigan statute also includes authorization for financial institutions to bring civil actions against persons for card replacement if a security breach of their database occurs. The bill is currently being developed for future vote.

Nevada Encryption Law

Nevada established its own encryption laws to enforce data confidentiality breaches at the state level. The Nevada encryption law (Statute 597.970), originally enacted on October 1, 2008 remained in effect until January 1, 2010, when the current law (Senate Bill 227) expanded the scope of the legislation by requiring all Nevada businesses to use encryption when data storage devices that contain personal customer data are moved beyond the "physical or logical controls" of the business.

Under the new law, **businesses must encrypt all personal information transferred by electronic transmission**. The new law requires compliance with the Payment Card Industry Data Security Standard—which helps organizations that process card payments prevent credit card fraud through increased control of data—businesses that accept payment cards. Although specific penalties for noncompliance with the Nevada statute are undefined, the law authorizes the state Attorney General to bring action to stop continuing violations.

Washington Encryption Law

Two bills pending in the Washington State legislature, Substitute House Bill 2838 and Senate Bill 6425, would authorize financial institutions to recover costs from data thieves who gain unauthorized access of customers' info.

Washington SB 6425 would also require businesses that collect or store personal information from payment cards to comply with payment card security standards established by the Payment Card Industry (PCI) security standards council.

Those standards mandate that while in storage, **the primary account number of payment cards must be protected by encryption**, hash indexes, truncation or index tokens and pads. Proposed Washington SB 6425 would require encryption for payment card data in transit and require either encryption or other data-masking measures for payment card primary account numbers while in storage.

www.echoworx.com

1.888.697.3246