PC Encryption Regulatory Compliance
Meeting Statutes for Personal Information Privacy

Gerald Hopkins

Cam Roberson

Personal Information at Risk
Legislating the threat

Since the 90s, personal data stored on the servers, desktops, and laptops of organizations has been under attack by unauthorized parties intent on identity theft and misuse. The need for protection of confidential consumer/ health information has always been recognized. However, an uneven response to the threat resulted in breaches of increasing size and frequency. Something had to be done.

Public outcry eventually compelled Federal and State legislators to adopt regulations to protect privacy. But loosely written laws intended to motivate organizations to secure personal data, such as the Health Insurance Portability and Accountability Act (HIPAA), failed to stem the rising tide of breach incidents due to a lack of specificity and enforcement.

In response, new and increasingly more stringent laws with greater specificity and enforcement provisions covering stored personal information (data at rest) have been enacted at both the Federal and State level. Multiple industries, from healthcare to financial services to retail, are directly impacted by one or more of these statutes.

Three Categories of New Law
Encryption and more

The first category includes laws that mandate data encryption of personal data at rest. Failure to comply may result in penalties (civil and criminal). Among these laws are HIPAA, Payment Card Industry Data Security Standard (PCI/DSS), and state laws in Massachusetts and Nevada (as well as proposed laws in Michigan and Washington).

A second category requires organizations not in compliance with encryption-oriented rules to notify those whose personal information may have been compromised. Encryption provides these organizations with a safe harbor, exempting them from notification and consequent negative publicity. 46 states have already passed such laws.

Finally, there are statutes that mandate protection of personal data without specifying how the organization should achieve that goal. While encryption is a proven means for protecting data, it is not a legislated requirement. These laws may also be vague with respect to enforcement and penalties. Examples include Gramm-Leach-Bliley, Sarbanes Oxley (SOX), and the Fair and Accurate Credit Transactions Act (FACTA). As with HIPAA, of course, the specificity of these laws may increase over time.

The remainder of this document looks at a number of key statutes (HIPAA, PCI/DSS, and laws enacted by Massachusetts, Nevada, and other states), how they affect organizations, and what organizations can do to meet compliance, avoid costly penalties and/or notification, and reduce customer defection.

HIPAA
Prescription for personal data security

Growing concern over the privacy of electronically stored patient health information (ePHI) led to the enactment of the Healthcare Insurance Portability and Accountability Act in 1996. The Act regulates Covered Entities (CEs), which include any health plans, healthcare clearinghouses, and healthcare providers that transmit health information electronically. Over the years, critics complained that HIPAA lacked specificity and, because penalties were

rarely levied, organizations took the position that compliance was discretionary.

The Interim Final Rule, which took affect in September 2009, added clear direction to HIPAA regarding breaches of unsecured ePHI, as well as very specific requirements for securing that data. CEs and their business associates that hold unsecured ePHI must notify affected individuals, the Department of Health and Human Services (HHS) and, in some cases, the media, when a breach occurs. The Interim Final Rule also stipulates monetary penalties, which can be significant. A violation due to willful neglect, for example, can result in fines of $50,000 per incident to as much as $1.5 million in a calendar year. CEs deemed compliant are relieved from having to notify in the event of a breach.

The Interim Final Rule specifies encryption and destruction as the means for rendering protected data unusable, unreadable, or indecipherable to unauthorized individuals [as defined by NIST Special Publication 800-111] Beachhead's SimplySecure™ Management System enables CEs to meet HIPAA requirements for encryption by enforcing encryption across their inventory of Windows & Mac PCs, Android tablets and phones, iPhones, iPads and USB storage devices.

The Final Rule has now become effective (March 26, 2013) which formalizes the contents of the Interim Rule and paves the way for stringent enforcement of penalties for violations of the act. Business Associates of these entities, frequently a source of data breach, are also subject to it's statutes. While there have already been many severe fines for many large and recognized offenders s clear that small entities will not escape enforcement of the rule.

> **excerpt from the HHS News Release January 2013 "HHS announces first HIPAA breach settlement involving less than 500 patients"**
>
> *The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.*
>
> *"This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." said OCR Director Leon Rodriguez. "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."*

SimplySecure™ further allows administrators to make data unusable or unavailable to users. It even anticipates future compliance requirements with the additional ability to destroy data remotely if an unauthorized individual gains access to a mobile device. A terminated employee or someone who had stolen a laptop with the password conveniently left with or near the computer could easily access encrypted data. SimplySecure™ can make that data unavailable.

Payment Card Industry Data Security Standard (PCI DSS)
Shopping for security

Developed and managed by the Security Standards Council and its founders, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed, or transmitted by merchants and other organizations. PCI DSS includes requirements for Protecting Cardholder Data and Implementing Strong

Access Control Measures.

Compliance is not an option for organizations covered by these requirements, as stiff penalties may be levied for failure to meet them. Merchants or processors can be fined up to $50,000 per day for non-compliance. And if cardholder data is compromised due to a security breach, an organization can face fines of up to $500,000 per incident, plus any fraud losses incurred from the use of compromised account numbers. Other costs include the cost of re-issuing compromised cards, as well as the cost of any additional fraud prevention and detection activities.

One of the major requirements in PCI DSS is to Protect Cardholder Data by rendering it unreadable anywhere it is stored (including data on portable media, in logs, and data received from or stored by wireless networks) using strong cryptography. PCI additionally requires that encryption keys be protected against disclosure and misuse, and that old keys be destroyed. SimplySecure™ provides strong cryptography. Organizations can easily enforce encryption of data on PCs enterprise-wide. LDD ships configured with government-approved 256-bit Advanced Encryption Standard (AES).

Also under Protecting Cardholder Data, PCI requires organizations to protect encryption keys from disclosure or misuse and carry out the mandated destruction of old keys. LDD escrows keys, allowing administrators to remotely destroy the local key, preventing data access to any designated PC.

Another major requirement within PCI DSS is to Implement Strong Access Control Measures. SimplySecure™ effectively addresses these requirements at the PC level. For example, PCI DSS calls for the immediate revocation of access for terminated users, and the removal of inactive user accounts every 90 days or less. By remotely destroying the local key, LDD can immediately remove access to these users. The organization can optionally choose to permanently remove access to sensitive data stored on a PC.

Additionally, under Implement Strong Access Control Measures, PCI includes a number of requirements related to user passwords. They must be changed every 90 days. They must be at least seven characters long and contain both numeric and alpha characters. New passwords must not be repeated for at least four cycles. All of these rules are intended to make hacking passwords more difficult. Unfortunately, they introduce behavior that too often defeats the intent, driving users to write down these difficult-to-remember passwords. (Studies have shown that 1 in 3 users do exactly that.[1]) Many are stored with the PC or nearby. Any unauthorized individual who has the password has access to the data, regardless of encryption. Should a laptop be lost or stolen, however, SimplySecure™ enables administrators to destroy the local PC key and prevent unauthorized access to that data.

Other PCI requirements for Implementing Strong Access Control Measures stipulate locking out users after no more than six login attempts. SimplySecure™ provides this capability in addition to other security responses by locking access to data, even if the user has the password, until cleared by the administrator. Another requirement sets lockout duration to 30 minutes or until an administrator enables the user ID, and forces users to re-enter their password after 15 minutes of inactivity. Only SimplySecure™ can provide these control measures to combat unauthorized PC data access.

Massachusetts and Nevada
Other States to Follow

Concerned by the rising level of identity theft and fraud, individual states are beginning to enact legislation to aggressively protect their citizens' personal information. One of the most notable is Massachusetts (home base for TJ Maxx, which experienced one of the largest personal data breaches in history in 2007). Taking effect January 1, 2010, a new state law [201 CMR 17.00] specifying data encryption of Massachusetts residents' personal

data is one of the strictest in the country.

The law requires any firm (regardless of where they are located) that is conducting business with Massachusetts 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, such as laptops.

Penalties can add up quickly. Organizations can be fined $100 per name, up to $50,000 per incident, for disposing of a computer with unencrypted personal data. A lost PC could lead to a fine of $5000 per incident. And failure to comply with the encryption laws leaves organizations subject to suit by the Massachusetts Attorney General with damages trebled for willing or knowing violation of the law.

Nevada passed similar personal data encryption laws, which also take effect on January 1, 2010. The law (NRS 603A) adds specificity to an existing encryption law and applies to any organization doing business in Nevada that collects an individual's first name or initial and last name plus Social Security number, employee identification number, driver's license number, or credit or debit card number or financial account number that has a security code. Because virtually every employer collects employee Social Security numbers, the law applies to all employers. In addition, the new law mandates compliance with PCI DSS for businesses that accept payment cards. NRS 603A requires businesses to disclose in writing any exposure of personal data to affected consumers. The disclosure process can be costly, but failure to disclose can open businesses up to civil and criminal actions.

Other states are following the lead of Massachusetts and Nevada, requiring businesses to proactively protect sensitive data with encryption and provide more substantial penalties for failure to do so, and exposing companies to general legal liability for data losses. Michigan, which has an existing law (Senate Bill 309) mandating disclosure of breaches, is considering more stringent legislation similar to Massachusetts, stipulating the use of encryption to protect personal data. Encryption legislation is also under consideration in Washington State.

SimplySecure™ allows organizations to enforce encryption to meet compliance with Massachusetts and Nevada privacy laws, and those states that pass data protection laws in the future.

States with Breach Disclosure Laws
46 states including District of Columbia, Puerto Rico, Guam, and the Virgin Islands

While Massachusetts and Nevada have taken the lead in securing personal information by delineating encryption of that data, 46 other states already have Breach Disclosure Laws on the books.

These laws are modeled after California's groundbreaking Security Breach Information Act (SB 1386) that took affect in July 2003. These laws mandate data protection of consumer data and, while encryption isn't necessarily specified, its use does offer a safe harbor for meeting disclosure requirements. SB 1386 doesn't impose fines or minimum prison sentences, but it does permit customers injured by a violation of the law to recover damages. The greatest threat, however, may be to the bottom line, as the cost of notification alone is estimated to cost a violating organization $202 per record, an increase of 2.5% from 2007 . Most importantly, data loss has considerable negative impact on a company's brand and reputation.

SimplySecure™ from Beachhead allows organizations to enforce encryption, the most often specified way for protecting personal data and meeting state breach disclosure laws. Organizations that encrypt personal data are typically not required to notify breach-affected individuals in the event that a PC or other device with personal information is lost or stolen, thereby avoiding media exposure, damage to their reputation, and financial loss.

Beachheads' SimplySecure™ Management System
Complete mobile data protection

SimplySecure™ enables organizations to enforce encryption of sensitive data on their inventory of mobile devices quickly, easily, and without significant IT burden or user impact. SimplySecure™ is delivered and managed through secure internet communications (via the "Cloud"), compliance can be achieved in literally one day. There is no need to locally install encryption on each mobile device and there is no investment or support necessary for IT hardware/software infrastructure. Finally, users have no involvement in the operation of the tool, so they continue to operate their device – whether theirs or the company's – in exactly the same manner. This innovative approach to encryption and data security provides compliance without impacting the productivity of employees.

Some laws and industry requirements go beyond encryption of personal data. An unauthorized person in possession of the password who can boot the PC can access encrypted data. SimplySecure™ provides the capability to destroy data (permanently and in some cases, recoverably) remotely if an unauthorized individual gains access to that data.

Beachhead invites you to learn more about the comprehensive protection offered the SimplySecure™ Management System, delivering unprecedented control and security of personal data on your inventory of mobile computing and communicating devices.

[1] Source: Nucleus Research, 2006

Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126
408.496.6936

Question, comments? Write Cam Roberson
croberson@beachheadsolutions.com