BEACHHEAD
Whitepaper

PC Encryption Regulatory Compliance

Meeting Statutes for Personal Information Privacy

Gerald Hopkins

Cam Roberson

April 2019

Legislating the threat

Since the time mankind invented written language some 5,000 years ago, it's likely that people began writing about things they tried to keep secret. Rather than hiding written material, people eventually invented systems of ciphers, or substituting different characters for each other. Consider the case of the Bronze Age (1500 B.C.) pottery maker who memorialized a pottery glaze recipe, on a clay tablet, using ciphers. Doubtless, the potter was worried about someone stealing his valuable information, and he did what he could to protect it. Some things never change: It's an old problem that has taken on new dimensions with the emergence of digital technology. 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, and financial information has always been recognized, but an uneven response to the threat resulted in breaches of increasing size and frequency. Something had to be done.

Public outcry eventually compelled government entities (both state and federal) to implement laws and regulations intended to protect private information. But loosely written laws and uneven enforcement failed to stem the rising tide of breach incidents. Private entities also took steps to try to address the growing threat, with mixed results.

In recent years, stringent and increasingly specific data protection laws and regulations (with strict enforcement provisions) have been enacted by government jurisdictions in the United States and internationally, as well as by private regulatory organizations. Many industries, from healthcare to financial services to retail, are directly impacted by one or more of these statutes. The sheer number of these laws and regulations, and their varied requirements, can seem daunting. But as these laws and regulations pertain to protecting data on endpoint devices, there is good news: Encryption is the commonly accepted mandated or recommended methodology of protecting data.

This whitepaper will address four categories of laws and regulations intended to protect digital data:

1) Laws enacted by the United States Federal Government;
2) Laws enacted by the 50 US states and US territories;
3) Regulations implemented by private regulatory entities;
4) Laws enacted by non-US entities that nevertheless have potential consequences for US companies.

The requirements of these many laws are varied, and the potential consequences of non-compliance can be severe.

1. United States Federal Laws and Regulations

HIPAA is a federal bellwether and provides guidance to auditors

The US government has enacted an array of laws and regulations intended to protect digital information (with the healthcare and financial services being the most notable industries affected). Central to the federal regulations within the healthcare industry is the Health Insurance Portability and Accountability Act, or HIPAA. The law has a long history of revisions and temporary provisions, and until recently caused a great deal of confusion in the healthcare industry. The law is long, sweeping in its implications, and its specific provisions can be as confusing as the law's name. However, the provision most pertinent to the protection of data is something called the "Security Rule." The Security Rule essentially delineates the manner in which the HIPAA Covered Entity (“CE”) protects patients’ electronic personal health information (“ePHI”).

The rule covers an array of ePHI issues, including physical security, transmission of data, and the protection of ePHI on endpoint devices including PCs, servers, smartphones, tablets, and removable storage. Somewhat surprisingly, the Security Rule does not specifically mandate the use of encryption for protecting ePHI on endpoint devices; rather, it considers encryption an "addressable requirement" under the law. In other words, an entity covered under HIPAA must be able to demonstrate that it has implemented measures that demonstrably and verifiably protect the data. Why is the law so vague on this point? It appears that the drafter of the Security Rule envisioned the possibility that security technology would continue to evolve, and that a specific encryption mandate might at some point become obsolete if a yet-unforeseen, better-protective technology later emerged. As of 2019, that unforeseen, better technology has not emerged, and encryption is the only viable technology available to comply with HIPAA's requirement, avoid embarrassing public disclosures of data breaches, and, most significantly, avoid the severe penalties imposed by the Department of Health and Human Services (the enforcement agency for HIPAA).

As a means to ensure that ePHI is protected through the extended chain of those who may have access to a CEs' ePHI, the law also extends to those defined as Business Associates ("BA") to the CE. Medical billing companies, transcription services, data storage and providers of technical services (e.g. MSPs) would all be considered BAs to their respective CE. To be clear, a BA is defined as an organization who has the ability to access a CEs' ePHI and not necessarily an organization that has accessed ePHI.

The federal government also has implemented several laws pertaining to the financial services and banking sectors, most notably Gramm-Leach-Bliley ("GLB"), Sarbanes-Oxley ("SOX"), and the Fair and Accurate Credit Transactions Act ("FACTA"). GLB requires financial institutions to protect non-public information through "administrative, technical and physical safeguards." As the law pertains to data at rest, encryption on endpoint devices is the only viable method of complying with the law. Similarly, FACTA requires financial institutions to maintain robust security plans aimed at reducing the risk of compromising consumers' financial data. Breaches of unprotected data result in mandatory public disclosure and potentially severe penalties. SOX's reason for being is different than those of GLB and FACTA: While those laws are intended to protect consumer information, SOX was enacted to ensure the integrity of financial data -- meaning the data should be accurate and complete for reporting purposes, safe from the threat of being altered and compromised. Again, encryption of such data on endpoint devices is the only current, viable method of complying with this law. You should be aware of the Federal Information Security Management Act of 2002. This law pertains to data security within federal agencies. The law relies on NIST Publication 800-53 for providing the framework by which federal agencies (and contractors) assess security risks, and encryption is referenced often as an example of appropriate technology for securing endpoint data.

Effective December 31, 2017, all US Department of Defense (DOD) contractors and subcontractors are required to have achieved NIST 800-171 compliance. NIST 800-171 compliance requires two-factor authentication, employee training, 24/7/365 network security monitoring, compliant cloud and local backup, policy generation, onsite support, technical secure engineering, patch management and testing, and ***device-level encryption.*** The bar is set extremely high and, borrowing from the HIPAA playbook, the DOD seeks to ensure these protections are held throughout the system. As such, contractors are forced to assign subs into two categories – those that will be compliant and those that won't – and then figuring out which compliant companies to grant the business that used to go to the non-compliant ones. In other words, contractors will be disallowed and in violation for awarding contracts to non-compliant players.

2. State Laws and Regulations

Each of the fifty US states and the territories (Puerto Rico, Guam, US Virgin Islands) have their own laws and regulations pertaining to the protection of sensitive, personal data. Some states – notably Massachusetts, New York, and Nevada – lead the way in this regard and enacted their own strong legislation protecting electronic data through encryption. More states have followed suit in recent years, also requiring encryption.

However, other states have a dizzying array of variations to their laws, particularly with regard to breach disclosure requirements: Some states only require disclosure if there is a reasonable belief that the breach is likely to cause actual harm. Other states require notice in the event of a breach regardless of the likelihood of actual harm. And there are many variations between the states on the timing of notice requirements based upon the number of affected individuals. Even the most diligent expert in the area of data privacy laws would have a hard time keeping up with the proliferation of state laws.

But there is some good news here: Each of the states' laws contain provisions to the effect that the statutes do not apply if the information in question was encrypted (provided the encryption key is not compromised), redacted, or in some other way rendered unusable. The easiest and most practical way to ensure compliance with all state data privacy laws is to simply deploy encryption across all endpoint devices. For now, encryption is the only reliable game in town.

3. Private Regulation of the Problem: Payment Card Industry Data Security Standard (PCI DSS); FINRA

Shopping for security

Recognizing the growth of electronic data, and understanding the severe consequence of data breaches (civil and criminal penalties, fines, public disclosure, etc.), certain industries have been particularly proactive trying to get ahead of the issue. The payment card industry is a leader in private regulation: 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 expense 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.

Also under the Protect Cardholder Data requirement, PCI compels organizations to protect encryption keys from disclosure or misuse and carry out the mandated destruction of old keys.

Another self-regulatory organization, the Financial Industry Regulatory Authority (FINRA) was formed in 2007 for the purpose of regulating and overseeing securities firms that do business with the public. FINRA regularly issues guidance and oversight regarding member compliance with applicable federal data protection regulations, including Securities Exchange Commission regulations and legislation such as the Fair Credit Reporting Act. We can expect to see more self-regulation by industry consortiums in an effort to proactively avoid running afoul of government regulators.

4. International Regulations

The world's strongest and most comprehensive data rules are found in the European Union's General Data Protection Regulation (GDPR), enacted in May of 2018. The intent of the law is to make data protection regulations across Europe uniform in scope and application. Many US companies continue to be surprised to learn that their compliance with GDPR is now a practical requirement of doing business in Europe. "Data Controllers" and "Data Processors" are covered by the law – Data Controllers (entities actually controlling the procedures and purpose of the data) have the most responsibility, while Data Processors (parties that process data at the direction of the Data Processor) also share compliance responsibilities. Classes of data protected by the law are broad and cover essentially any piece of data that can be used to identify an individual. This could be a name, email address, phone number, IP address, device name, etc.

If you are a US-based company (whether a Data Processor or Data Controller) and are controlling or processing the personal data of an individual located in the European Union, you are likely subject to the provisions of GDPR. One of the most pertinent provisions of GDR requires that organizations implement measures that provide adequate protection of data – including the encryption of personal data. Like HIPAA, GDPR has provisions for publicly shaming non-compliant organizations. And the shaming can be the least of the potential problems. Penalties for breaches of personal data can be severe: Non-compliance can result in fines of up to 10,000,000 EUR, or up to 4% of "annual turnover" (annual revenue).

Encryption for All Businesses

Regardless of industry or size

Encryption has become the de facto compliance standard to protect data on PCs and mobile devices. Effective encryption shields organizations from devastating breaches and violations, fines and penalties and public outcry and reputation tarnishing. This whitepaper covers myriad sources for such compliance mandates, the implementation specifics of which are often admittedly unspecific or seemingly discretionary. HIPAA, over the last two years, has become the bellwether compliancy standard and is often cited for specific guidance from auditors across all compliancy disciplines. Encryption is almost always prescribed by auditors as an interpretation of more loosely defined data security standards wherever sensitive data is concerned.

For the last of those who believe these new and more stringent requirements apply only to the largest of organizations, think again. The requirements are moving from enterprise through SMB, and the vehicle for its enforcement is coming in the form of compliancy questionnaires. For SMBs within the ecosystems of larger enterprises, effective and wholly up-to-date data security is now a requisite of conducting business. SMBs that don't feature security in line with what enterprise questionnaires are specifically looking for will find it more and more difficult – if not already impossible – to win new business. At the same time, legacy providers grandfathered into these business relationships will need to meet these same requirements in order for their services to be retained. And, considering the reality that many SMBs are dependent on a few or even a single large-size client for the lion's share of their revenue, the prospect of receiving a security assessment questionnaire from a key client that an SMB is unprepared to answer should be a frightening one.

Beachhead's SimplySecure™ Management System

Enforced, managed and proven compliance tool

SimplySecure™ enables organizations to enforce encryption of sensitive data on their inventory PCs and mobile devices quickly, easily, and without significant IT burden or user impact. SimplySecure is delivered and managed through secure internet communications (via the cloud) and 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, end 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.

As additional data protection, SimplySecure protects remote, sensitive data under conditions where encryption alone cannot. Remote data access control or data elimination can protect if an unauthorized individual gains access to that data. This can help you protect your data if a password is compromised or if a remote employee with the ability to access your PC quits or is terminated.

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 PCs and mobile devices.

BEACHHEAD

Beachhead Solutions Inc.
1150 S. Bascom Avenue
San Jose, CA 95128

Question, comments? Write
info@beachheadsolutions.com