Received 9 February 2016
Accepted 9 February 2016

Information doesn't always want to be free

An overview of regulations affecting information security

H. Frank Cervone
University of Illinois at Chicago, Chicago, Illinois, USA

Abstract

Purpose – Information professionals are increasing called upon to provide access and services for information that, by its nature, must be restricted to certain uses or classes of individuals. This paper aims to explore the six major compliance regulations in the USA that information professionals should have a basic understanding of to manage a restricted information environment effectively.

Design/methodology/approach – This paper is a general review of laws and requirements in the USA related to information security that may affect information professionals in their work.

Findings – The world of information security is complex and there are multiple laws, guidelines and standards that apply. For information professionals managing or deploying digital repositories or information archives, all of these need to be considered because plans and systems are being developed. Information professionals will increasingly be called upon to lend their expertise to emerging preservation problems related to restricted data, so understanding the basics of information security law is a requirement to successful information practice.

Originality/value – This is the first general overview of this area of information practice.

Keywords Information security, FERPA, FISMA, HIPAA,
Laws related to information security in the USA, Secure repositories

Paper type General review

Although informatics and data science generally tend to focus on providing access to information, there is another side to providing information that is increasingly coming into play for many information professionals. Especially in the commercial sector, in specialized agencies and in educational institutions, certain types of information are required to be protected and only made available to those with appropriate access rights. Unlike traditional debates that focus on intellectual freedom or a philosophical approach to providing open access to research, there are several classes of information where access must be restricted and this is governed by law.

As information professionals, it is important for us to have a basic understanding of the major issues that govern these protected types of data. Whether providing access to information or curating the information that is under our care, ensuring that we adhere to the rules that govern information dissemination requirements is an important, but often misunderstood, aspect of our work.

In the USA, there are six major information compliance regulations, two of which are more commonly known in the information professional community (HIPAA and FERPA) and four regulations that are less well known (Sarbox, FISMA, GLBA and PCI-DSS).

Digital Library Perspectives
Vol. 32 No. 2, 2016
pp. 68-72

2059-5816
DOI 10.1108/DLP-02-2016-0009

Health Insurance Portability and Accountability Act

The most widely known of all the regulations that affect information security, the Health Insurance Portability and Accountability Act (HIPPA) is not primarily about information security at all. The original Act, passed in 1996, is mainly focused on improving the portability and continuity of health insurance coverage for employees, particularly when they change or leave jobs.

This is implemented in five distinct components of the law, known as titles, with the most significant to information professionals being *Title II*, the Administrative Simplification (AS) provisions. The original idea behind the AS provisions was to enact requirements that would establish national standards for the transmission of electronic health-care information as well as establish unique identifiers for individual providers, health insurance plans and employers across the USA. Over the years, the law has been changed and expanded and today represents one of the most complex regulations related to information security.

HIPAA requirements for information security are defined in various "rules" including:

- *The privacy rule*: This governs the use of an individual's protected health information (PHI). PHI is a broad concept as it includes all information about a person's health status, how health care has been provided and how health care has been paid. Put another way, PHI is generally considered to be any part of a person's medical record and related payment history.
- *The security rule*: This defines the three types of safeguards required for compliance. These are categorized as administrative, physical and technical standards. Within each standard, there are required and "addressable" standards. Required specifications are neither optional nor open to interpretation. This is in contrast to the "addressable" standards which can be implemented by organizations in a more flexible manner to meet the requirements of the organization.
- *The unique identifiers rule*: This requires that the unique identifier of a health-care provider (i.e. doctor, clinic and hospital) be used in all transactions related to the provider.
- *The transaction and code sets rule*: This defines the specific ways in which various types of electronic health-related data are transmitted between systems. That is, this rule defines the metadata schemes used for the transmission of all types of health and health-related records.
- *The enforcement rule*: This sets fines and penalties for violations of HIPAA rules. In addition, this rule defines the procedures for investigation of HIPAA violations.

HIPAA is particularly relevant to information agencies in a medical or related environment as any repository used for storing patient or research data related to people receiving health care must conform to HIPAA rules. In most cases, this means that specialized software rather than traditional repository software, such as DSpace Fedora, EPrints, or Greenstone, must be used to comply with the requirements. As the fines for HIPAA violations are quite severe, securing PHI data is to be taken quite seriously.

FERPA (Family Educational Rights and Privacy Act)

Older than HIPAA, the Family Educational Rights and Privacy Act (FERPA) was passed into law in 1974. Unlike HIPAA, the focus of FERPA is clearly on information. Specifically, FERPA is about ensuring the privacy of student information. For students under 18, the Act

gives parents specific rights to see information related to their child's education. However, once a student turns 18, these rights generally transfer to the student. At this point in most cases, a parent no longer has the ability to view these records. However, this is not true if the student is still a dependent of the parents. Interestingly, if a student is married, their spouse has no inherent rights to view their spouse's educational records.

In contrast to HIPAA, FERPA does not require an educational institution to keep or maintain records unless there is an outstanding request to inspect the records. On the other hand, the institution is required to maintain a record of all of the requests to view education records. And additional twist is that FERPA only applies to institutions that receive funds from the US Department of Education.

As one can imagine, one of the major problems facing those trying to implement FERPA guidelines is simply understanding what those guidelines are. Given that the applicability of rules in given situations may vary depending on the circumstances and who is involved, many institutions have layered their own interpretations of the FERPA guidelines onto their local enforcement of the policy in an effort to simplify understanding of what use is permissible and what is not.

Information agencies that are charged with storing FERPA data face a somewhat daunting challenge. The rules for determining what falls under the guidelines and what does not are relatively straightforward but subject to interpretation and individual's decisions. For example, a school is not allowed to disclose personally identifiable information (PII) about a student without the student's consent. But, FERPA allows "school officials" with a "legitimate educational interest" to see that PII. In addition to several other exceptions related to law enforcement and tax evasion, it is also possible for an institution to provide unrestricted access to PII if it is "directory information" which includes the:

> […] student's name, address, e-mail address, telephone listing, photograph, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended, grade level or year and enrollment status (undergraduate or graduate; full-time or part-time (Family Policy Compliance Office, 2016a).

Because of the potentially invasive nature of some of this information, many institutions allow students to suppress some or all of the "directory information" from release upon request of the student.

Clearly, any repository that contains student data needs to provide great flexibility to accommodate the many different contexts in which FERPA data could and should be provided. As with HIPAA, software designed specifically for this purpose is required.

FISMA (Federal Information Security Management Act of 2002)

The Federal Information Security Management Act (FISMA) was first adopted in 2002. It was subsequently revised and renamed in 2014 to the Federal Information Security Modernization Act. This Act is directly related to information security. It requires all federal agencies to develop, document and implement a security program for all information managed by the agency. One of the provisions of this law is that it requires an annual review of the security program by the agency.

One of the major reasons this Act is of interest to information professionals outside the US Federal Government is because of how it affects other organizations. Organizations that interact with federal agencies often find themselves subject to the same FISMA requirements as the federal agency itself. As a consequence, an

information organization may need to ensure is that its information systems and repositories comply with federal requirements, such as the FIPS 200 standard which is described in the National Institute for Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" (National Institute for Standards and Technology, 2013).

In general, the FISMA requirements outline what are considered by many to be the best practices in regard to information security. For this reason alone, it is useful for information professionals to be, at least, casually acquainted with the NIST standards.

Sarbox (Sarbanes-Oxley Act)

The Sarbanes-Oxley Act (Sarbox), which was passed in 2002, is another Act that is not directly related to information or its protection, yet affects security practice. The primary purposes of this law were to regulate financial practices and corporate governance in the wake of several well-documented accounting and corporate governance failures such as Enron National Public Radio (2016), WorldCom Romero and Atlas (2002) and Arthur Andersen Brown and Dugan (2002). A quick review of the law will reveal that most of its provisions are related to governing and regulating accounting and related functions.

Where the Act is of interest to information professionals is that it requires *all* organizations, regardless of size, to have a defined, credible and detailed information security plan. Although development of this plan is often left to information technology personnel, other information professionals have significant roles to play given the multitude of perspectives and use cases they bring to the discussion.

GLBA (Gramm–Leach–Bliley Act)

The Gramm-Leach-Bliley Act was passed in 1999 and, like Sarbox, is not concerned directly with information security but rather focuses on the regulation of the banking, insurance and investment industries. A provision of the law known as the "Safeguards Rule" requires organizations affected by the Act to develop a security plan to protect their clients' nonpublic personal information. The intent is similar to what HIPAA does for health information but GLBA focuses on financial information.

As with FISMA, probably the biggest impact of GLBA on information professionals is that its provisions may work their way into the expectations organizations under the governance of the Act may have in regard to their partners' security plans.

PCI DSS (Payment Card Industry Data Security Standard)

Finally, the Payment Card Industry Data Security Standard (PCI DSS) regulates the way credit and debit card information can be used within an organization. PCI DSS is unique, as it is not a legal requirement or regulation but rather a proprietary standard developed by the payment card industry itself. This standard has very demanding requirements for how payment card information is collected, transmitted and stored. Additionally, it requires regular audits of information systems that collect or store payment card information. Fines for violations of the standards can be very severe, often starting at minimum of $750,000 per violation.

Where this standard comes into play for information professionals is in those organizations where payment card information is collected. If customers or patrons pay for services or fees with a payment card, the organization must comply with the PCI DSS guidelines. Given the complexity of the regulations and the significant consequences of getting it wrong, many organizations outsource the collection and management of

payment card information to third-party vendors, thereby shifting the responsibility for implementation and compliance to the outsourced organization.

Summary

The world of information security is complex and there are multiple laws, guidelines and standards that apply. For information professionals managing or deploying digital repositories or information archives, all of these need to be considered as plans and systems are being developed. Although in many organizations, there has not been a big demand for some of these specialized applications, such as a HIPAA-compliant repository, that is changing. As more researchers using these protected data sources fall under requirements to preserve their data for the scientific and research record, information professionals will increasingly be called upon to lend their expertise to these emerging preservation problems.

References

Brown, K. and Dugan, I. (2002), "Arthur Andersen's fall from grace is a sad tale of greed and miscues", *Wall Street Journal*, available at: www.wsj.com/articles/SB1023409436545200 (accessed 4 February 2016).

Family Policy Compliance Office (2016a), "FERPA general guidance for students", available at: http://familypolicy.ed.gov/content/ferpa-general-guidance-students (accessed 30 January 2016).

National Institute for Standards and Technology, (2013), "Security and privacy controls for federal information systems and organizations- 800-53 A (Rev. 4)", available at: doi:10.6028/NIST.SP.800-53Ar4 (accessed 04 February 2016).

National Public Radio (2016), "Fall of enron", available at: www.npr.org/news/specials/enron/ (accessed 04 February 2016).

Romero, S. and Atlas, R.D. (2002), "Worldcom's collapse", available at: www.nytimes.com/2002/07/22/us/worldcom-s-collapse-the-overview-worldcom-files-for-bankruptcy-largest-us-case.html (accessed 04 February 2016).

Further reading

Family Policy Compliance Office (2016b), "FERPA for school officials", available at: http://familypolicy.ed.gov/ferpa-school-officials?src=ferpa (accessed 1 February 2016).

Health and Human Services (2016a), "Health information privacy", available at: www.hhs.gov/hipaa/ (accessed 30 January 2016).

Health and Human Services (2016b), "Privacy", available at: www.hhs.gov/hipaa/for-professionals/privacy/ (accessed 30 January 2016).

Corresponding author

H. Frank Cervone can be contacted at: fcervone@uic.edu