Health Systems (2014), 1–13

www.palgrave-journals.com/hs/

ORIGINAL ARTICLE

A tale of two standards: strengthening HIPAA security regulations using the PCI-DSS

Mark Gaynor[1], Catherine Bass[1] and Bryan Duepner[1]

[1] *Saint Louis University, St. Louis, U.S.A.*

Correspondence: Mark Gaynor, School for Public Health & Social Justice, Saint Louis University, 3545 Lafayette Ave, Salus Center, Room #361, MO, St. Louis, 63104, U.S.A.
Tel.: +(314) 977-8304;
Fax: (314) 977-8150;
E-mail: mgaynor@slu.edu

Received: 27 February 2013
Revised: 2 July 2013
2nd Revision: 10 October 2013
3rd Revision: 29 November 2013
4th Revision: 17 February 2014
5th Revision: 7 April 2014
6th Revision: 8 July 2014
Accepted: 8 July 2014

Abstract
This paper both illustrates the inadequacy of current Health Insurance Portability and Accountability Act (HIPAA) regulations in protecting health-care information and proposes a more cohesive strategy to protect such information based on the organizational model that undergirds the Payment Card Industry Data Security Standards (PCI-DSS). The evidence indicates that the industry consortium model used to develop the PCI-DSS works rapidly and effectively. The success of these standards suggests that their strengths provide a favorable base from which to develop a robust set of standards to enhance information security within health care. A national organization consisting of industry representatives that is devoted to creating a more comprehensive and less vague set of security standards is required to protect health-care information more effectively than is possible under the current HIPAA approach.
Health Systems advance online publication, 22 August 2014;
doi:10.1057/hs.2014.17

Keywords: HIPAA; PCI-DSS; standards; security; patient information; compliance

Introduction

Information privacy and security has been and continues to be a 'pain point' in the health-care industry, as discussed in the recent literature (Herzlinger *et al*, 2013), (Kokolakis *et al*, 2001; Kumar & Lee, 2011) and in the popular media (Sack, 2011; Hickins, 2014; King, 2014; Parker, 2014). In the United States, privacy and security standards in health care are defined by the Health Insurance Portability and Accountability Act (HIPAA, 2013). When compared with similar security standards in other industries, such as the Payment Card Industry Data Security Standards (PCI-DSS) (PCI, P.-H, 2013), HIPAA only vaguely specifies the need to protect health-care information and does not specify how such information should be protected. Unfortunately, as health information technology (HIT) continues to advance without a robust and specific set of security standards, the health-care industry is likely to experience even more security breaches than the financial sector because of HIPAA's weak security standards and the slow nature of change in government standards/policies.

Information security is defined by the US Congress under Title 44, Chapter 35, as 'protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide' (Congress, U.S., 2011) data integrity, confidentiality, and availability. Health-care information privacy and security involves interactions among information collection and dissemination, information technology, the patient's expectation of privacy, and the current regulatory environment. There were more than 31,000 breaches of health-care information between September 2009 and May 2011; this volume both indicates

the extent to which the health-care industry is becoming a more prominent target for information theft and highlights the ineffectiveness of HIPAA standards in protecting health-care information (Goedert, 2011).

As credit card use in health-care increases, health-care organizations that have financial arrangements with patients (i.e., customers who pay with credit cards) are increasingly falling under the payment card industry (PCI) umbrella as credit card vendors. Thus, these organizations must comply with the PCI-DSS as well as with HIPAA. Fortunately, the purpose of these two standards is similar, namely, to protect consumer information. However, whereas HIPAA has been described as a 'swing and a miss' and a 'miserably executed' standard (Conn, 2011), the PCI-DSS are arguably more effective than HIPAA regulations and can serve as a reference model for the standardization and enforcement of new health-care information security standards. A new strategy is proposed to create a set of standards to protect health-care information based on the organizational model that serves as the foundation for the PCI-DSS and the detailed technical specifications that describe how to protect this information. This strategic plan will help create a logical and cohesive set of standards and enforcement procedures that ensures the privacy and security of health-care information that is required under HIPAA. Forming a health-care industry consortium that is similar to the PCI Security Standards Council can drive the creation of these new standards.

This position paper presents an introductory discussion of the potential enhancement of HIPAA regulations by devising a strategy based on the organizational structure of the PCI Security Standards Council to create a more comprehensive set of standards that better protect the privacy and security of health-care information. The intention is to propose an improved organizational model for health-care privacy standards that would allow the standards to evolve with HIT. The next section provides an overview and analysis of both the PCI-DSS and the HIPAA regulations, which is followed by a comparative discussion of the strengths and weaknesses of the PCI-DSS and HIPAA regulations. Following this discussion, the similarities between the PCI-DSS and HIPAA regulations are illustrated. The subsequent section discusses how to use the strengths of the PCI-DSS to strengthen the HIPAA rules. The paper then discusses a set of past security breaches and illustrates how following the PCI-DSS might have prevented these breaches of patient privacy. Finally, the last section addresses certain potential difficulties in the suggested strategy.

Security standards overview and analysis

This section provides a summary of the PCI-DSS, which instruct organizations that accept credit cards on how to protect customer data. This section also summarizes the HIPAA regulations that describe which, whose, and how patient health information should be protected. It provides an analysis of the strengths and weaknesses of both the PCI-DSS and HIPAA.

PCI-DSS overview

In 2004, the PCI-DSS (summarized in Table 1) were established through a cooperative effort involving Visa, Discover, MasterCard, the Japan Credit Bureau (JCB), and American Express (PCI-Self-Assessment, S. S. C., 2009; PCI-Navigating, S. S. C., 2010; PCI-Standard, S. S. C., 2010). The intent of this group was to develop a set of standards for properly securing credit card information in terms of access, accountability, and security. Governed by a private entity, the PCI-DSS apply to anyone who processes and stores credit card information. As a private member entity, the PCI Security Standards Council also maintains the right to revoke member privileges – including payment card processing and other relevant activities – in the event of non-compliance.

The PCI-DSS in Table 1 apply to all member organizations. The PCI-DSS have a tiered organization with four levels, and each level is based on the number of annual transactions within an organization. Compliance Level 1 is for organizations that process over 6 million e-commerce transactions per year, whereas Level 4 compliance is for businesses with fewer than 20,000 such transactions annually. Higher levels, or large organizations, have a more demanding timeline to comply with the PCI-DSS requirements, in order to protect the large number of consumers utilizing their services. In addition to these requirements, the Security Standards Council provides insight and recommendations regarding the proper application of the standards and a multitude of supporting documents designed to ease the implementation process.

PCI-DSS strengths

The organizational structure of the PCI-DSS Security Standards Council and its standards has many strengths that include the focused collaborative culture of the Council, easy access to the standards, and effective deterrents for non-compliance.

The PCI Security Standards Council acts as the driving force for security within the industry and was established solely for the purpose of improving data security and integrity within the credit card industry. The presence of a micro-focused governing body enables the use of a single set of rules for the entire industry, decided upon by the industry, which reduces the number of procedural variations. This approach is highly responsive to industry demands and reinforces the ideas of standardization and interoperability as evidenced by the success of the PCI-DSS and organizations with a similar focus, such as the Internet Engineering Task Force (IETF, 2014) that standardizes the Internet or the W3C (2014) that standardizes the World Wide Web.

The PCI-DSS were established through the collaboration of the individual members and strengthen the security of not only the individual organizations but also the industry as a whole, which increases customer satisfaction and confidence. All stakeholders have the same goals and criteria for success. In this way, the member organizations

Table 1 Summary of PCI-DSS goals and a brief description of the specific requirements

PCI-DSS goals and requirements
Goal 1 – Build and maintain a secure network
Requirement 1 – Install and maintain a firewall configuration
Establish firewall and router standards that restrict inbound and outbound communication with the cardholder data and document protocols and configurations
Requirement 2 – Do not use vendor-supplied defaults for security parameters
Always change vendor-supplied defaults, including passwords, protocol community strings, and elimination of superfluous accounts prior to installation on a network
Goal 2 – Protect cardholder data
Requirement 3 – Protect stored data
Minimize data storage, including authentication data, by developing a data retention and storage policy consistent with industry regulations
Requirement 4 – Encrypt the transmission of data across open, public networks
Use strong encryption and security protocols to protect sensitive data during transmission over open, public networks; never send unencrypted data over public messaging technologies (email, IM, chat and so on)
Goal 3 – Maintain a vulnerability management program
Requirement 5 – Use and regularly update antivirus software
Use antivirus software on all systems that could be afflicted by malicious software and ensure that they are current, running, and capable of generating audit logs
Requirement 6 – Develop and maintain secure systems and applications
Ensure all systems are up-to-date and establish a process for vulnerability identification within all systems. Develop change control procedures and document their use
Goal 4 – Implement strong access control measures
Requirement 7 – Restrict access to data on a need-to-know basis
Limit data/system access to only those who require such information by establishing an access control system that restricts access based on developed criteria
Requirement 8 – Assign a unique ID to each person with access
Assign all users a unique ID before allowing access to system/data while also using at least one authentication method for local access and multiple levels for remote access
Requirement 9 – Restrict physical access to data
Use appropriate facility controls to limit and monitor physical access to systems, including procedures designed to distinguish between employees and visitors, such as a visitor log
Goal 5 – Regularly monitor and test networks
Requirement 10 – Track and monitor all network resource and data access
Establish a process for linking system components to individual users and for automating audit trails with respect to these components. Secure audit trails and review component logs daily while retaining logs for at least 1 year
Requirement 11 – Regularly test security systems and processes
Test for the presence of wireless access points at least quarterly and run internal and external vulnerability scans after any significant network change. Use intrusion-detection systems to monitor all traffic and alert personnel to any security compromises
Goal 6 – Maintain information security policy
Requirement 12 – Maintain a policy that addresses information security
Establish and maintain a security policy addressing daily operational security procedures, technology usage policies, information security responsibilities, employee security awareness training, employee screening, and an incident response plan

understand that security is a common concern that is better addressed as an industry, even if they are competing with one another in the marketplace. Historically and logically, the finance industry spends more on IT than any other industry (Gartner, 2010) and has been and should be a leader in information security because a large-scale failure to secure this information would result in irreparable harm to the industry itself (Informationweek, 2002; Wisegate, 2013).

The PCI-DSS are easy to access and understand because they are contained within a 75-page document and are concisely written in language that is specific to and understood by their audience (PCI, P.-H, 2013). Moreover, although there are additional documents to facilitate understanding, these supporting documents simply serve as appendices intended to clarify the central document for those who might struggle with the technical language in the actual standards or who would like to know the intent of particular standards. In addition, the PCI-DSS are easy to find and download online (PCI, P.-H, 2013).

The tiered architecture of the PCI-DSS has advantages over the flat HIPAA structure. As larger organizations have greater resources and more data, it is logical that they should meet the PCI-DSS requirements more quickly.

Conversely, smaller organizations are not weighed down with the undue burden of fulfilling PCI-DSS requirements as fast as organizations with more resources. Despite this apparent advantage over HIPAA, there is also a disadvantage associated with the tiered system of the PCI-DSS, discussed below.

PCI-DSS weaknesses

The tiered system of the PCI-DSS, again, is configured such that smaller organizations do not have to meet security requirements as fast as larger organizations. This design leads to smaller organizations with less secure environments that are more susceptible to a security breach.

Although the PCI-DSS are strong, breaches do occur, such as the recent loss of information at Target (Luckerson, 2013). In general, information security for organizations seems more reactive than proactive; for example, most antivirus software only works on viruses that have previously been discovered (Perlroth, 2012). Hackers who are interested in obtaining this information seem to be a step ahead of those who are protecting the information. The cost of protecting data must be balanced against the risk of a data compromise and the costs of such a compromise, should it occur.

HIPAA overview

Established by Congress in 1996, HIPAA is designed to safeguard protected health information (PHI) (HHS-PHI, U.S.-G.-Dept, 2013) from access when such information is created, exchanged, or stored by covered entities (i.e., health-care organizations). PHI includes any identifiable information about a patient that might be linked to a specific individual, including the patient's name, date of birth, and medical record number. HIPAA is separated into the Privacy Rule and the Security Rule (Pabrai, 2003). The Office of the National Coordinator (ONC, U.S.-G, 2013) defines the privacy and security of health-care information (HHS-Privacy, U.S.-G.-Dept, 2013) via HIPAA as follows:

- The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities (e.g., hospitals, clinics, skilled nursing facilities, and rehabilitation centers) and their business associates and gives patients an array of rights with respect to that information. The Privacy Rule is also balanced such that it permits the disclosure of health information required for patient care and other important purposes.
- The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of PHI.

This paper is primarily interested in the Security Rule because its intent is similar to that of the PCI-DSS goals, that is, defining how to protect personal information.

The HIPAA legislation sought to define information accessibility and security on a need-to-know basis. All health-care providers that have access to and store PHI, including health plans (e.g., insurance companies), health-care providers (e.g., clinics, hospitals), and health-care clearinghouses, are covered by HIPAA (HIPAA-Consumers, U.S. D. O. H. A. H. S., 2011). Table 2 summarizes HIPAA regulations and highlights important safeguards associated with HIPAA. Table 2 was created from the many separate documents that contain the HIPAA regulations, with the associated document referenced for each category. Note in Table 2 that 'IS' stands for 'implementation specifications,' that is, the specific requirements included under the general standard heading. In addition, any implementation specifications that are italicized are classified as 'addressable implementation specifications.' These specifications have particular stipulations related to their implementation.

HIPAA strengths

HIPAA provides rules that are required for improved information security that is highly specific to the health-care industry. Patients benefit the most because HIPAA regulations give them control over the information contained in their medical records, including the ability to authorize who can view their health information (ONC-Hie, 2013). This facet of HIPAA is particularly important because of the 'Minimum Necessary Requirement' (HHS-MNR, U.S.-G.-Dept, 2014), which allows access only to those who require patient information to provide appropriate treatment. This protocol helps ensure that treatment is provided in a safe and efficient manner while also restricting unnecessary access. In this way, HIPAA prohibits the inappropriate use and disclosure of PHI.

Although they are complex in nature, these safeguards are in place across the country, and all health-care employees are required to understand HIPAA regulations and their role in protecting health information.

HIPAA weaknesses

HIPAA has many weaknesses, including the difficulty of finding the correct document. Conversely, the 'PCI has 73 pages of requirements in one document, including all introductions, workflow charts, samples, appendices and other material. The actual standards themselves cover 46 pages. HIPAA covers at least 9 separate documents, covering 125 to 237 pages' (Atomic, I, 2009). Although the foregoing is only one example, this complexity has led to HIPAA being described as inaccessible due to the number and length of the relevant documents (HIPAA-Admin, U.S. D. O. H. A. H. S., 2005; HIPAA-Entities, U.S. D. O. H. A. H. S.-C., 2005; HIPAA-Physical, U.S. D. O. H. A. H. S., 2005; HIPAA-Policy, U.S. D. O. H. A. H. S., 2005; HIPAA-Technical, U.S. D. O. H. A. H. S., 2005; HIPAA-Consumers, U.S. D. O. H. A. H. S., 2011). This reduced accessibility impairs the abilities of both individuals and organizations to understand and properly adhere to HIPAA regulations. This challenge becomes more problematic when viewing the issue as a matter of scope because HIPAA

Table 2 Summary of HIPAA standards and associated requirements

HIPAA Standards and Implementation Specifications
*Administrative Safeguards (*Hipaa-Admin, U.S. D. O. H. A. H. S., 2005)
Standard 1 – Security management process
IS: Risk analysis, risk management, sanction policy, information system activity
Standard 2 – Assigned security responsibility
Standard 3 – Workforce security
IS: Authorization, workforce clearance procedure, termination procedures
Standard 4 – Information access management
IS: Isolate clearinghouse functions, access authorization, establishment, and modification
Standard 5 – Security and awareness training
IS: Security reminders, protect from malicious software, log-in monitor, password management
Standard 6 – Security incident procedures
Standard 7 – Contingency plan
IS: Data backup plan, disaster recovery plan, emergency operation plan
Testing/Revision Procedures, Application/Data Criticality Analysis
Standard 8 – Evaluation
Standard 9 – Business associate contracts and other arrangements
*Physical safeguards (*HIPAA-Physical, U.S. D. O. H. A. H. S., 2005)
Standard 1 – Facility access controls
IS: Contingency operations, facility security plan, access control/validation procedure, maintenance records
Standard 2 – Workstation use
Standard 3 – Workstation security
Standard 4 – Device and media controls
IS: Disposal, media re-use, accountability, data backup, and storage
*Technical safeguards (*Hipaa-Technical, U.S. D. O. H. A. H. S., 2005)
Standard 1 – Access control
IS: Unique User ID, emergency access procedure, automatic logoff, encryption/decryption
Standard 2 – Audit controls
Standard 3 – Integrity
IS: Mechanism to authenticate EPHI
Standard 4 – Person or entity authentication
Standard 5 – Transmission security
IS: Integrity controls, encryption
*Organizational requirements (*Hipaa-Policy, U.S. D. O. H. A. H. S., 2005)
Standard 1 – Business associate contracts
Standard 2 – Requirements for group health plans
*Policies and procedures and documentation requirements (*Hipaa-Policy, U.S. D. O. H. A. H. S., 2005)
Standard 1 – Policies and procedures
Standard 2 – Documentation

does not differentiate among organizations based on size or number of patients. As a result, smaller organizations with less manpower and fewer resources must navigate through the same ocean of information at the same pace as larger organizations.

According to Chris Bennington, a HIPAA specialist with a law firm in Cincinnati, Ohio, HIPAA laws are difficult to discern even for health-care workers (Rhea, 2007) because of their vagueness and lack of clarity. The focus of the HIPAA regulations is not on the mandates themselves but on the thought process used to address information security. This mindset leads to an emphasis on what to do, but explanations of how to adhere to specific standards are absent. When requirements are presented, no recommendations or guidance for implementation is provided to improve adherence to the standards. Furthermore, the wording within the documents lacks urgency; requirements are frequently presented as suggestions rather than being treated as compulsory.

As Stephen Stewart, CIO of the Henry County Health Center in Southeast Iowa, has stated, 'in health care, the only time anybody does things is if there is a mandate' (Conn, 2011). Contrary to what HIPAA defines as requirements, these addressable specifications demand that the organization document that it has examined the standard in terms of its necessity and applicability to the organization. The nature of these specifications allows the organization to interpret standards as it sees fit, deciding whether they are relevant to information security, which leads to inconsistent application of the regulations. Thus, these

'standards' are not standardized in the classic sense of the term because two organizations could produce quite different solutions for a single security or privacy issue.

Another limitation of HIPAA is its ineffective enforcement in the event of non-compliance and the difficulties inherent in providing for appropriate deterrents to non-compliance. The nature of HIPAA punishment for non-compliance is frequently to determine whether non-compliance is based on malicious intent or simple negligence (Mcquarrie, 2007). Proving malicious intent, however, is difficult in an environment in which human error can occur. If the intent is not deemed malicious, punishment is frequently in the form of a fine or is left to the discretion of the non-compliant organization. This approach can lead to the termination of the individual responsible for the breach but not necessarily to improving the training and knowledge of the employee base to enhance compliance with the statute, because most incidents are considered isolated events.

Because enforcement is lax, there is little incentive for health-care organizations to adhere strictly to HIPAA standards. Indeed, one patient advocacy group expressed surprise when dual million-dollar fines were levied on Cignet Health and Massachusetts General for HIPAA violations (Zigmond, 2011).

A universal deterrent for most public industries would be the negative publicity surrounding security breaches, as illustrated by the breach of as many as 40 million credit and debit card accounts at Target (Luckerson, 2013). Similarly, in the health-care industry, the primary incentive to maintain adequate security is simply to prevent the community from associating a breach with the health-care organization because 63% of the costs of a HIPAA breach result from lost business (Goedert, 2011).

The Health Information Management Systems Society has estimated that 'only 56% of respondents who experienced a security breach notified the patients involved' (Solutions, K. F., 2008). In response, certain states have enacted legislation, such as California's, 2002SB 1386, that specifically dictates that any consumer whose personal information might have been accessed or acquired by an unauthorized individual must be notified by the respective organization, regardless of industry.

In addition, the Department of Health and Human Services is not required to be notified unless a breach affects 500 or more individuals (Goedert, 2011), with one caveat: incidents do not have to be reported if adequate encryption is used to protect electronic PHI. This provision seeks to avoid the lost profits that would result from publication of a breach. Unfortunately, because this provision represents the sole incentive, there remains little impetus for the health-care industry to adopt high-end, expensive information security measures to protect patient privacy.

The limitations cited above likely reflect the conditions under which HIPAA was originally developed because the political process is not always responsive to rapidly evolving technology and user needs. Political in origin, HIPAA was heavily influenced by lawmakers who were neither experts in HIT nor directly involved in the health field, which limited the effective scope of HIPAA legislation (Cunningham, 2000). According to Deven McGraw, a lawyer heading the Health Privacy Project at the Center for Democracy and Technology, the unforeseen growth of HIT has meant that HIPAA is lagging behind the times (Conn, 2011). The process to create and update HIPAA was and still is legislatively driven, a situation that is inherently slow due to the need for different political parties to deliberate to reach consensus. The lack of an apolitical, independent certification body further hinders any amendment of existing standards because there is no lobbying group to advocate for further legislation. In combination with the fluid nature of the governing body, this situation produces an overall lack of accountability due to HIPAA's weak enforcement, changing politics, and the absence of an overall audit standard within the health-care industry based on patient and information volume.

HIPAA and PCI-DSS similarities and differences

PCI-DSS and HIPAA have many similarities because both are designed to provide guidance for implementing security technology that protects user privacy. The most obvious difference between the PCI-DSS and HIPAA is that HIPAA is designed to protect health-care data and patient privacy, whereas the PCI-DSS are focused on credit card data, which have different attributes than health-care information. For example, personalized health-care information is critical for effective emergency medical care. As a result, the attributes for an effective set of security standards for health care differ from those for financial information because medical providers must have rapid access to information, such as drug allergies for providers that may not have a previous therapeutic relationship with the patient and may not be able to obtain the patient's consent.

One important difference is that the PCI-DSS have a greater focus on the consequences of non-compliance than the lax and somewhat subjective system in HIPAA (Wafa, 2009). Under the PCI-DSS, a lack of compliance can lead to significant fines and the possibility that the Security Council will revoke an organization's ability to process credit card data. The punishment for a breach is frequently proportional to the degree of non-compliance, which enhances the incentives for member organizations to both understand and properly address the standards.

Figure 1 and Table 3 highlight the similarities and differences between the PCI-DSS and HIPAA, and are based on an analysis of Tables 1 and 2, including the supporting documents that are referenced.

Figure 1 summarizes the relationship between individual HIPAA rules and the PCI-DSS (HIPAA, 2013; PCI, P.-H, 2013). For the HIPAA standards, those labeled with an 'A' are administrative standards, 'P' indicates physical standards, 'T' represents technical standards, and 'D' stands for

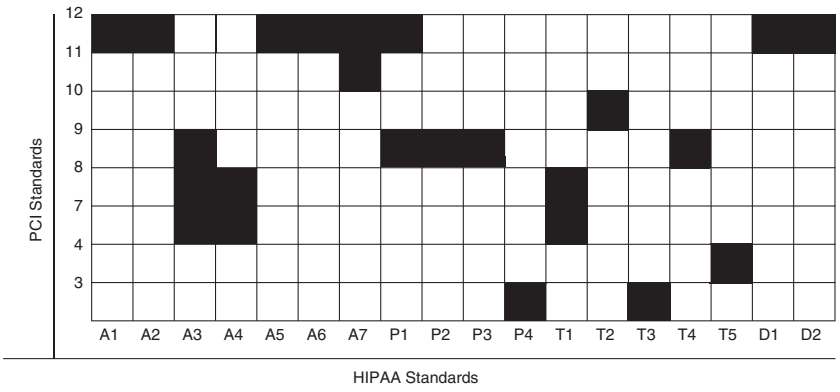

Figure 1 Summary of the relationship between PCI-DSS and HIPAA.

Table 3 Summary of non-overlapping PCI-DSS and HIPAA standards

PCI-DSS	
Standard 1	Firewall configuration
Standard 2	Change vendor-supplied default parameters
Standard 5	Antiviral software use
Standard 6	Secure system development and maintenance
HIPAA	
Regulation A8	Evaluation
Regulation A9	Business associate contracts and other arrangements
Regulation O1	Business associate contracts
Regulation O2	Requirements for group health plans

policy, procedure, and documentation standards. This figure provides a useful summary of the similarities between HIPAA and the PCI-DSS. Filled-in boxes indicate overlaps in which the standards are similar. For example, the language and intent of PCI-DSS Requirement 3 are similar to those of HIPAA Standard P4, and HIPAA Standard T1 covers those measures discussed in PCI-DSS Requirements 7 and 8, which is why their respective boxes are filled in.

Conversely, Table 3 (HIPAA, 2013; PCI, P.-H., 2013) presents standards that are distinct for each set of requirements. This table helps demonstrate the unique policies of each of the respective standards and is useful for showing how the PCI-DSS and HIPAA can be combined into a more robust set of security standards. For the HIPAA standards, those labeled with 'A' are administrative standards, and those labeled with 'O' are organizational standards. It is notable that the distinct HIPAA standards only apply in the administrative and organizational areas.

Prior to the relatively recent industry-wide shift toward implementing electronic health records (EHRs), the prevalence of paper-based record keeping in health care created a barrier between the PCI-DSS and HIPAA. Although the two sets of standards shared similar purposes with respect to protecting consumer information, the lack of congruence between their methodologies impeded synergy between the two programs. With the proliferation of EHRs, however, the implementation and application of the PCI-DSS and HIPAA have begun to converge due to their shared, explicit goal of protecting personal electronic information for the benefit of both the health-care consumer and the health-care industry. Both standards boast a variety of methods for protecting and securing electronic information.

The similarities are highlighted using general terms in the bullet list provided below. These terms are derived from the International Organization of Standards (ISO, 2010) 17799: 2005 Code of practice for information security management, the National Institute of Standards and Technology (NIST, 2013) SP 800 series of standards, the recommendations from the IETF Request for Comment 2196 Site Security Handbook (IETF-Security, 1997), and Principles of Information Security (Whitman & Mattord, 2005). These traditional security methods are present in the PCI-DSS with greater clarity than in HIPAA:

- *User authentication*: This method seeks to ensure that the users are who they say they are, including by assigning a unique user ID to be presented when accessing electronic information. This method includes linking a specific username to a specific password (Morris & Thompson, 1979). The password can be something the user knows (password), something the user has (ID card), or something that is part of the user (biometrics such as fingerprints), and it includes the development of system protocols for changing one's user information (PCI-DSS Requirement 8, HIPAA Technical Safeguards).
- *Access authorization*: This method seeks to determine who has access based on established criteria defining 'need-to-know' by job classification and is directly linked to user authentication; moreover, this method aids in assigning the level of information access that any individual should receive. One example of a system that combines authentication and authorization is the Kerberos infrastructure developed at MIT (Miller *et al*, 1987). Access can be provided based on who the user is (identification based) or what the user is doing (role-based authorization) (PCI-DSS Requirements 7, 8, and 9, HIPAA Technical Safeguards).

- *Encryption* (Schneier, 1996): This method includes standards for when and how to encrypt data for storage and transmission to prevent unlawful access by an outside party (PCI-DSS Requirement 4, HIPAA Technical Safeguards).
- *Physical access* (Russell *et al*, 2011): This method includes facility and workstation access, including the security of the actual building and reservoirs of information (PCI-DSS Requirement 9, HIPAA Physical Safeguards).
- *Audit controls* (Weber, 1998): This method seeks to track data access along with rules to specify how to protect data to ensure that data are accessed only by authorized users (PCI-DSS Requirement 10, HIPAA Technical Safeguards).
- *Policies and procedures*: This method includes rules and incident response plans for the proper protection and security of information and for execution in the event of a breach or disaster (PCI-DSS Requirement 12, HIPAA Policy Requirements).

In addition to these methods, organizations working with both credit card and health information must be held accountable to both sets of standards, as there are established consequences for failure to uphold information security to protect the privacy of financial and health information. HIPAA and the PCI-DSS both focus on information security, integrity, and protection; however, their means of accomplishing their goals differ, and these differences influence the relative effectiveness of each standard.

Using PCI-DSS strengths in HIPAA

Establish a certification body

Although the spirit of these two sets of standards is similar, they have been implemented differently. Nevertheless, their similarity provides a foundation that facilitates the use of the strengths of one to enhance the other (Gikas, 2010). The first step in creating additional standards to strengthen HIPAA is to develop and establish an appropriate certification body. In the case of the PCI-DSS, this goal was achieved through the collaboration of representatives from MasterCard, Visa, American Express, Discover, and the JCB and resulted in the establishment of a joint security council (PCI, P.-H., 2013). To achieve the same end for HIPAA would require input from a wide array of health-care stakeholders, including the Centers for Medicare and Medicaid Services (CMS), the American Medical Association (AMA), and the National Institutes of Health (NIH), as well as market leaders in health IT (e.g., health security and EHRs). This approach would endeavor to create an authorized body whose purpose would be to extend the privacy and security rules of HIPAA in a timely manner and ensure appropriate compliance with these expanded standards.

Implicit in this proposed approach is the creation of a council consisting of experts in the health-care field (e.g., experts in health informatics/security, medicine, administration, finance, and public policy) that would oversee the major developments and revisions to the existing HIPAA regulations. To implement a new strategy, a PCI Security Standards Council representative should be included to help ensure cohesiveness between the two standards in light of the presence of credit card information within health care. The cooperation of the individual segments of the health-care field is integral to the success of any improved policy that would be generated by this certification body because of the breadth and complexity of the health-care industry. By accomplishing these goals, the creation of the council would also incentivize and encourage non-traditional health-care workers to participate in council activities to further improve the impact of these new standards and strengthen the entire health-care community.

The establishment of a certification body and the revision of the HIPAA regulations might serve to increase the extent of standardization based on the implementation of a tiered system. These tiers would be developed based on organizational characteristics including size, patient load, the type of information, and the status of the electronic health systems. This tiered arrangement would facilitate an increased awareness by individual health-care organizations of the particular regulations that affect them, how quickly these regulations must be complied with, and the consequences of non-compliance.

Reassess accessibility and reduce ambiguity

One of HIPAA's major weaknesses is its inaccessibility and its cumbersome nature, whereas the PCI-DSS are contained within a single document that can easily be found online. The first step in improving HIPAA accessibility would be to compile all its individual documents into a single master document and to remove redundancies in the process. During consolidation, careful consideration should be employed to ensure that the minimum standards and information to be controlled are explicitly enumerated with recommendations for proper implementation. In addition, methods to implement higher security standards should be provided for the benefit of organizations that are interested in exceeding the minimum requirements.

The new master document should next be placed on the homepage of the newly developed governing body website, as well as on the websites of its constituents (e.g., CMS, AMA, NIH). Another option would be to contact major search engines to ensure that these new standards would be a top response to related queries, which would improve document accessibility. One good example of contextually aware searching is the process of searching for drugs on Google that provides a knowledge tree of information.

Following the specification of the minimum standards, the focus should shift to a re-evaluation of the tone and scope of HIPAA, beginning with the removal or redefinition of addressable implementation standards.

The addressable standards provide excessive flexibility, which inhibits interoperability and standardization across the health-care industry. At the organizational level, these addressable standards give institutions the freedom not only to implement these standards as they see fit but also to determine their general relevance. The presence of these non-mandatory standards reduces the impact of the legislation as a whole and, as such, should be redressed. If such standards are determined to be appropriate, they should be made mandatory.

Although the tone of HIPAA might be considered ineffective given the scope of the standards, the same cannot be said about the PCI-DSS, which are all treated as mandatory. For example, the PCI-DSS require that no computer with credit card information be directly connected to the internet (PCI, P.-H., 2013). Along with an appropriate tone, the PCI-DSS also provide insight and direction for proper implementation. John Christly, manager of IT security and HIPAA security officer from Memorial Health Care System, has even posited that using the PCI-DSS can offer a clear idea of the controls and actions that must be taken to provide security (Degaspari, 2010). He added, 'the stance we took in trying to figure out how to make a secure network for the credit card terminals is the same stance you take to try to figure out how to secure where you are taking care of the patient' (Degaspari, 2010). Considering the widespread use of credit cards in health care, adhering to a stricter set of standards might result in 'killing two birds with one stone.'

Part of this strength is derived from the PCI-DSS's explicitness in defining the particular groups of individuals to whom the requirements apply through its tiered (multi-layered) system based on organization size and the volume of credit card use. Under this system, the requirements and recommendations change based on the data type and the number of data transactions that occur (PCI, P.-H., 2013). This approach allows for improved standardization across different-sized organizations based on the belief that higher risk demands stricter compliance and verification obligations.

Appropriate deterrents

Although both sets of standards address the consequences of non-compliance, their methodologies and punishments differ. HIPAA is more concerned with the motive behind non-compliance. By contrast, the PCI-DSS are more concerned with the knowledge that an event occurred and focuses on the steps, or lack of steps, taken to prevent an incident of breach. These drastically different ideologies regarding non-compliance and incident management are reflected in the punishments delivered to the organization or individual responsible for an information breach. Although the HIPAA ideology may be appropriate for individual mistakes, it is ineffective at the organizational level. As malfeasance is particularly difficult to prove, HIPAA is frequently lax in its punishments, which incentivizes some organizations not to follow the standards properly.

The PCI-DSS ideology, however, does not focus on intent and punishes according to the lack of adherence to the standards. This focus on the 'letter of the law' allows organizations to be more aware of what actions will require punishment and what they can do to avoid it. With adherence-based punishment, the best way to avoid punishment is simply to follow the standards set forth by the Security Standards Council. As a result, organizations can avoid fines, loss of reputation, and perhaps even a reduction in the scope of services. In the event that these standards are not followed, enforcement is necessary to ensure future compliance. An established governing body is essential to enable appropriate enforcement and to ensure consistency across the industry, which HIPAA currently lacks.

According to an article in Health Care Financial Management, 'There is also some question as to whether regulators might be providing a significant disincentive to self-report HIPAA breaches that are uncovered during internal audits. A series of graduated warnings or penalties might be a more appropriate strategy with respect to HIPAA breaches. But guidelines regarding such incidents have not yet been developed' (Sarrico & Hauenstein, 2011). These rules can describe the level of non-compliance that would trigger a certain level of punishment. Furthermore, a punishment progression plan should be developed in the case of repeated non-compliance. A critical aspect of enforcement should also include mandating that patients be informed as to whether their privacy is compromised, along with details about what information was exposed and what steps should be taken to re-secure their personal information. In addition, in the event of larger-scale incidents, the community as a whole and the individual stakeholders must be notified. This publicity, and the possibility of losing business, revenue, and customer confidence, might be considered a more effective deterrent than explicit punishments. Moreover, the combination of these factors would serve to further deter non-compliance while emphasizing the need for proper security measures.

Breaches

Several security scenarios are presented and analyzed below. In each of these scenarios (Tables 4–6), proper implementation of the more explicit guidance of the PCI-DSS could have prevented a breach.

Potential problems

Widespread policy changes in the health-care security arena have the potential to create problems. Costs must be considered in terms of the implementation of the PCI-DSS and the explicit description of minimum requirements. These costs would include security technology implementation costs (e.g., hardware, software) and personnel costs associated with additional hires, training, and the time necessary to implement the new standards. In addition, because HIPAA does not possess a governing body and remains politically influenced, amending the

Table 4 Summary of breach at Family Health Center

Event description

Family Health Center, located in Virginia, announced in March 2010 that they had been made aware of the inappropriate disposal of patient information. Boxes containing patients' health histories, surgeries, insurance, and bank account information were found in a dump (Center, Family Health, 2011).

Cause of breach – Improper disposal of patient information

Compromised HIPAA standard	*Relevant PCI-DS standard*
Physical safeguard: Standard 4 – Device and medical controls (addressable) ● Govern the receipt and removal of hardware and electronic media that contain EPHI in and out of a facility in addition to the movement of these items within the facility ● Govern proper handling of electronic media, including receipt, removal, backup, storage, reuse, disposal, and accountability	*Requirement 3.1* ● Minimize data storage and develop a data retention and disposal policy *Requirement 9.6* ● Physically secure all paper and electronic media that contain data *Requirement 9.10* ● Destroy all media containing data when they are no longer required ● Render data on electronic media unrecoverable so that data cannot be reconstructed

Lessons to be learned

Organizations must not only properly dispose of medical information but also keep an up-to-date inventory of paper-based medical records

Table 5 Summary of breach at Lincoln Medical and Mental Health Center

Event description

In 2010, Lincoln Medical and Mental Health Center, located in the Bronx, New York, and its billing vendor sent out seven CDs containing PHI via FedEx. Holding more than 130,000 records and completely unencrypted, the data on these disks were compromised when the envelope was lost (Mcmillan, 2010). As a result, Lincoln and Siemens have stopped sending sensitive information via overnight delivery companies

Cause of breach – Unsecure transfer of PHI

Compromised HIPAA Standard	*Relevant PCI-DS standard*
Technical safeguard: Standard 5 – Transmission security (addressable) ● Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network ● Implement a mechanism to encrypt EPHI whenever deemed appropriate *Physical safeguard: Standard 4 – Device and medical controls (addressable)* ● Govern the receipt and removal of hardware and electronic media that contain EPHI in and out of a facility as well as the movement of these items within the facility ● Govern proper handling of electronic media, including receipt, removal, backup, storage, reuse, disposal, and accountability	*Requirement 4.1* ● Use strong encryption methods to secure data that are transmitted over open networks. Although the data were not being electronically transmitted, they were being physically transmitted; for this reason, the 'spirit' of the requirement still holds *Requirement 9.7* ● Maintain strict control over internal or external distribution of any media that contains data classified as confidential ● Send the media by secured courier or another delivery method that can be accurately tracked *Requirement 9.9* ● Maintain strict control over the storage and accessibility of media containing data

Lessons to be learned

The use of simple encryption and proper methods for securing and transferring data would have easily prevented this breach. These measures could include the employment of a secure courier and mandating password protection and authentication to access all data regardless of the type of media. As shown above, the HIPAA safeguards that were violated were the addressable standards discussed above relative to the limitations of HIPAA

Table 6 Summary of breach at AvMed Health Plans

Event description

In late 2009, AvMed Health Plans, located in Florida, experienced a type of information breach that is far too common in the health-care industry. In this particular instance, AvMed claimed that over 1.2 million records were exposed when two laptops were stolen directly from their corporate offices (Barrett, 2010); laptop thefts are considered one of the most common forms of health-care information breach. Although the company would not specify whether the data were encrypted, it expressed confidence that the risk of fraudulent use was low

Cause of breach – Laptop theft from within the office

Compromised HIPAA standard	*Relevant PCI-DS standard*
Technical safeguard: Standard 1 – Access control ● Implement policies and procedures that allow access only to those persons or programs that have been given access rights	*Requirement 3.1* ● Develop a data retention and disposal policy; limit storage amount and retention time to that which is required
Technical safeguard: Standard 4 – Person or entity authentication ● Implement procedures to verify that a person or entity seeking access to EPHI is who he or she claims to be	*Requirement 8.3* ● Incorporate two-factor authentication for remote access to the network
Technical safeguard: Standard 5 – Transmission security (addressable) ● Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network ● Implement a mechanism to encrypt EPHI whenever appropriate	*Requirement 9* ● Restrict physical access to cardholder data
Physical safeguard: Standard 4 – Device and medical controls (addressable) ● Govern the receipt and removal of hardware and electronic media that contain EPHI in and out of a facility as well as the movement of these items within the facility ● Govern proper handling of electronic media including receipt, removal, backup, storage, reuse, disposal, and accountability	

Lessons to be learned

This scenario demonstrates the risks inherent in using laptops as mobile workstations, particularly for information storage purposes. Although accessing information is essential, storing this information on a laptop is risky. Instead, organizations should focus on allowing remote access via multiple forms of authentication. In addition, leaving laptops or any other transportable device unattended is an exercise in poor judgment that should be addressed specifically within the security standards

legislation may prove difficult. In part, this difficulty is due to the turnover of elected representatives and the associated changes in congressional priorities, including the emphasis on health care. Even with an impetus to amend HIPAA, the legislative process is time-consuming, and implementation of major decisions is susceptible to substantial delays.

Another potential problem is related to the increased complexity associated with the necessary development of a tiered system of standards across a wide array of health-care institutions (e.g., home health institutions, skilled nursing institutions, laboratories, and multi-hospital organizations). Within the PCI Council, most of the member organizations behave similarly. This similarity facilitates simplification because there are fewer variables to consider. Conversely, health care involves numerous and diverse considerations. Although the overall goal of health care is to improve the health of individuals, this goal can be accomplished in myriad ways compared with those associated with credit card transactions.

In addition to the variability found within the health-care industry, the issue of organizational and industry buy-in related to the proposed changes is a topic of concern. The problem of buy-in is related to the possible costs and complexity associated with the discussed PCI-DSS/HIPAA hybrid and the general resistance to change, particularly when the change will result in a more punitive model. Mandating improved compliance might affect the bottom lines of these organizations, making them hesitant to support any wide-scale reform, particularly if increased security costs might impact their ability to provide health-care services.

Conclusions

This paper provides a brief overview of the PCI-DSS developed and maintained by a consortium of industry members and the HIPAA regulations passed by Congress. It examines the strengths and weaknesses of each of these sets of standards and regulations and investigates the similarities between the PCI-DSS and HIPAA. It suggests how the strengths of the PCI-DSS might be leveraged to build a better set of standards to protect information based on the HIPAA privacy and security rules that do not

contain sufficient technical detail or direction. As suggested above, incorporating the PCI-DSS and ideology to enhance the privacy required by HIPAA is likely to produce substantial improvements in both security (particularly in terms of increased standardized clarity and improved implementation) and enforcement. The industry consortium model of standardization is faster and more effective than the government-regulated HIPAA approach. As illustrated in the examples of information breach, HIPAA is ineffective in certain areas because it does not explicitly state how to protect patient information. Because the PCI-DSS have stronger wording, they require less interpretation, and the information breaches described above might have been prevented under the PCI-DSS. The final section of the paper discusses the concern that implementation of the PCI-DSS would be prohibitively expensive. It can be argued, however, that the risks and danger posed by security breaches and/or general vulnerabilities outweigh these costs. A phased approach that emphasizes implementation of the highest yield standards would be a cost-effective approach and would also allow organizations to generate the greatest impact while expending the smallest number of resources. This approach would also facilitate improved security, compliance, and enforcement, and would successfully address a worrisome issue for patients.

Acknowledgements

The authors wish to thank Michael Berger, Neil Gaynor, Tracy Omer, Cindy LeRouge, and the Area Editor for helpful comments and editing.

References

Atomic, I. (2009) HIPAA vs. PCI: Compare and contrast security standards. [WWW document] http://blog.atomicinc.com/2009/06/19/hipaa-vs-pci-compare-and-contrast-security-standards/ (accessed 16 October 2011).

BARRETT L (2010) AvMed breach exposes 200,000 customers' Info [Internet]. Foster City, California: QuinStreet Inc. [WWW document] http://www.internetnews.com/security/article.php/3864946/AvMed±Breach±Exposes±200000±Customers±Info.htm (accessed 16 October 2011).

California. (2002) Privacy of personal information. *SB 1386*. C. Senate.

Center, F. H. (2011) HIPAA at 15 some provisions still a work in progress. [WWW document] http://www.privacyrights.org/data-breach-asc?title=Family±Health±Center (accessed 19 January 2014).

Congress, U.S. (2011) Title 44, Chapter 35, Subchapter III, Section 3542. 44. U. Congress.

CONN J (2011) HIPAA at 15 some provisions still a work in progress. Modern Healthcare. [WWW document] http://www.modernhealthcare.com/article/20110822/MAGAZINE/308229962 (accessed 19 January 2014).

CUNNINGHAM R (2000) Old before its time: HIPAA and e-health policy. *Health Affairs* **19**(**6**), 231–238.

DEGASPARI J (2010) Staying ahead of the curve on data security: securing patient data in a changing healthcare landscape. *Healthcare Informatics* **2**(**10**), 32–36.

GARTNER. (2010) *Gartner Perspective: IT Spending 2010* Gartner, Stamford, CT.

GIKAS C (2010) *Information Systems Security: A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards*. Catapult Technology, Bethesda, MD.

GOEDERT J (2011, Aug 2011) Unraveling data breaches: your organization just uncovered a large breach of protected health information. What happens now? Health Data Management. [WWW document] http://www.healthdatamanagement.com/issues/19_8/unraveling-health-care-data-breaches-42886-1.html (accessed 19 January 2014).

HERZLINGER R, SELTZER M and GAYNOR M (2013) Applying KISS to health care information technology. *IEEE Computer* **46**(**11**), 72–74.

HHS-MNR, U.-G.-D. (2014) Minimum necessary requirement. [WWW document] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html (accessed 19 January 2014).

HHS-PHI, U.-G.-D. (2013) Protected Health Information (PHI). [WWW document] http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/underhipaa.html (accessed 19 January 2014).

HHS-Privacy, U.-G.-D. (2013) Health information privacy. [WWW document] http://www.hrsa.gov/healthit/toolbox/healthitimplementation/implementationtopics/ensureprivacysecurity/ensureprivacysecuritySSS_2.html (accessed 27 July 2013).

HICKINS M (2014) Medical Devices Can Lead to Breaches. *The Wall Street Journal*.

HIPAA. (2013) Health Information Privacy, HIPAA main web page, HHS.

HIPAA-Admin, U. S. D. O. H. A. H. S. (2005) *HIPAA Security Series. Security Standards: Administrative Safeguards*. Centers for Medicare and Medicaid Services, Washington DC.

HIPAA-Consumers, U. S. D. O. H. A. H. S. (2011) *Health Information Privacy: For Consumers.* HIPAA-Consumers, U. S. D. O. H. A. H. S, Washington DC.

HIPAA-Entities, U. S. D. O. H. A. H. S.-C. (2005) *HIPAA Security Series. Security 101 for Covered Entities*. Centers for Medicare and Medicaid Services, Washington DC.

HIPAA-Physical, U. S. D. O. H. A. H. S. (2005) HIPAA Security Series. Security Standards: Physical Safeguards, Centers for Medicare and Medicaid Services, Washington DC.

HIPAA-Policy, U. S. D. O. H. A. H. S. (2005) HIPAA Security Series. Security Standards: Organizational, Policies and Procedures and Documentation Requirements. Centers for Medicare and Medicaid Services, Washington DC.

HIPAA-Technical, U. S. D. O. H. A. H. S. (2005) HIPAA Security Series. Security Standards: Technical Safeguards, Washington DC.

IETF. (2014) The internet engineering task force. [WWW document] http://www.ietf.org/ (accessed 1 January 2014).

IETF-Security. (1997) *Site Security Handbook*, Internet Engineering Task Force.

INFORMATIONWEEK. (2002) Spending Shortfall – Despite threats of hacking an cyberterrorism, security spending remains tight. *Information Week*.

ISO. (2010) Information technology – security techniques – code of practice for information security management. *International Organization for Standardization*. 17799:2005.

KING R (2014) Hospitals face many challenges protecting health records from cyberattack. *The Wall Street Journal*.

KOKOLAKIS S, GITZALLIS D and KATSIKAS S (2001) Why we need standardisation in healthcare security. *Studies in Health Technology and Informatics* **69**: 7–12.

KUMAR P and LEE H-J (2011) Security issues in healthcare applications using wireless medical sensor networks. *Sensors* **12**(**1**), 55–91.

LUCKERSON V (2013) Target breach shows you can be a victim of cybercrime at a brick-and-mortar store. [WWW document] http://business.time.com/2013/12/20/target-credit-card-breach-shows-expansion-of-cybercrime/ (accessed 1 January 2014).

MCMILLAN R (2010) New York hospital loses data on 130,000 via FedEx. Computerworld. [WWW document] http://www.computerworld.com.au/article/351659/new_york_hospital_loses_data_130_000_via_fedex/?eid=-6787 (accessed 19 January 2014).

MCQUARRIE D (2007) HIPAA criminal prosecutions: few and far between. *HEALTH L. PERSP.*

MILLER SP, NEUMAN BC, SCHILLER JI and SALTZER JH (1987) *Kerberos Authentication and Authorization System*. P. A. T. Plan, MIT, Boston, MA.

MORRIS R and THOMPSON K (1979) Password security: a case history. *Communications of the ACM* **22**(**11**), 594–597.

NIST. (2013) *Computer Security Standards*. National Institute of Standards and Technology, Washington DC.

ONC-HIE. (2013) Health Information Exchange (HIE). [WWW document] http://www.healthit.gov/HIE (accessed 19 January 2014).
ONC, U.-G. (2013) HealthIT.gov – office of the national coordinator. [WWW document] http://www.healthit.gov/ (accessed 19 January 2014).
Pabrai U (2003) *Getting Started with HIPAA*. Premier Press, Boston, MA.
Parker A (2014) House votes to increase security measures on health care exchanges. *The New York Times*. New York.
PCI-Navigating, S. S. C. (2010) *Navigating PCI Data Security Standard*. PCI-Navigating, S. S. C, Wakefield, MA.
PCI, P.-H. (2013) PCI security standards council. [WWW document] http://www.pcisecuritystandards.org/ (accessed 19 January 2014).
PCI-Self-Assessment, S. S. C. (2009) *PCI Self-Assessment Questionnaire D*. PCI-Self-Assessment, S. S. C., Wakefield, MA.
PCI-Standard, S. S. C. (2010) *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures v.2*. PCI-Standard, S. S. C., Wakefield, MA.
Perlroth N (2012) Outmaneuvered at their own game, antivirus makers struggle to adapt. *The New York Times*.
Rhea S (2007) Clooney and hospital prying eyes. Experts wonder if incident will expose HIPAA weakness. *Modern Healthcare* **37**(**41**), 10.
Russell M, Kendig J and Philpott D (2011) *Guide to Physical Security Planning and Response for Hospitals, Medical, Long Term Care Facilities*. Government Training, Longboat Key, FL.
Sack K (2011) Patient data posted online in major breach of privacy. *The New York Times*. New York.
Sarrico CA and Hauenstein J (2011) Can EHRs and HIEs get along with HIPAA security requirement? *Healthcare Financial Management* **65**(**2**), 86–90.
Schneier B (1996) *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, New York, NY.
Solutions, K. F. (2008) *HIMSS analytics report: security of patient data, healthcare information and management systems society*, HIMSS, Chicago, IL.
Wafa T (2009) How the lack of prescriptive technical granularity in HIPAA has compromised patient privacy. *North Illinois University Law Review* **30**(**3**), 531–552.
W3C. (2014) World wide web standards. [WWW document] http://www.w3.org/ (accessed 1 January 2014).
Weber R (1998) *Information Systems Control and Audit*. Prentice Hall, Upper Saddle River, NJ.
Whitman M and Mattord H (2005) *Principles of Information Security*, 2nd edn, Thomson Learning, Mason, Ohio.
Wisegate. (2013) Building a winning case for your security budget. Wisegate Community Blog. [WWW document] http://blog.wisegateit.com/2013/10/16/building-a-winning-case-for-your-security-budget/ (accessed 1 January 2014).
Zigmond J (2011) HIPAA fine is a first. Modern Healthcare. [WWW document] http://www.modernhealthcare.com/article/20110228/MAGAZINE/110229939 (accessed 19 January 2014).