HIPAA and ISO/IEC 27001

Implement Once, Comply Many

bsi.

...making excellence a habit.™

HIPAA and ISO/IEC 27001

Implement Once, Comply Many

Abstract

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) Security legislation is a requirement for all healthcare organizations designated as "Covered Entities," along with their business associates and their subcontractors. ISO/IEC 27001 is the international standard for information security management. This paper compares these two standards to show how ISO/IEC 27001 can facilitate meeting multiple regulations and exceed the requirements under HIPAA. ISO/IEC 27001 provides a holistic process, thereby reducing the risk, resources and administrative burden that come with managing multiple silos of information.

Background on HIPAA and ISO/IEC 27001

HIPAA was enacted as a broad Congressional attempt at healthcare reform. Initially introduced in Congress as the Kennedy-Kassebaum Bill, the landmark Act was passed in 1996 with two objectives:

- To ensure that individuals would be able to maintain their health insurance between jobs. This is the "Health Insurance Portability" part of the Act. It is relatively straightforward, and has been successfully implemented.
- To ensure "Accountability" for those entities that hold patient information. This section is designed to safeguard the security and confidentiality of patient information/data. In addition, it mandates uniform standards for electronic data transmission of administrative and financial data relating to patient health information.

The HIPAA Privacy Rule provides federal protection for individually identifiable protected health information (PHI) held by covered entities and their business associates. It specifies a series of administrative, physical and technical safeguards to assure the confidentiality, integrity and availability of electronic protected health information.

The HIPAA Omnibus rule that went into effect on September 23, 2014 makes it clear that business associates (of covered entities) and their subcontractors are now directly responsible for HIPAA compliance.

Additionally, Health Information Technology for Economic and Clinical Health Act (HITECH), brings additional security challenges as government encourages and offers incentives for entities to use Electronic Health Records (EHRs) to improve quality and lower costs. The Office of the National Coordinator for Health Information Technology (ONC) developed the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information

The new Health Insurance Exchange (HIE), which launched in October 2014, will lead to a large number of people entering personal income and medical history data online. While the exchanges themselves are not considered covered entities under HIPAA, the insurance companies are. Under the HIE organizations, healthcare professionals and patients will be allowed to access patient data electronically.

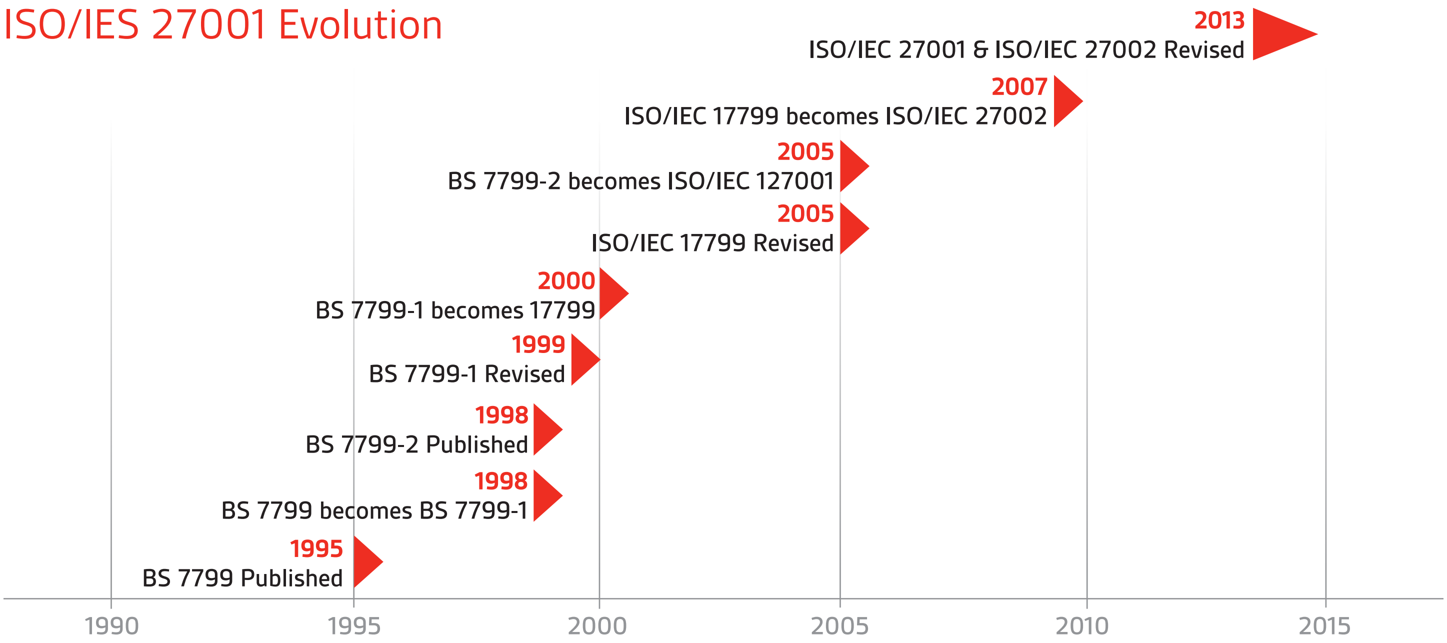
HIPAA/HITECH non-compliance can result in large fines. The increasing numbers of breaches and fines that have been publicized have caught the attention of the public. On September 23, 2014, Leon Rodriguez, director of the Department of Health and Human Services' OCR, said he expects that OCR "will leverage more civil penalties," as part of their audit program. The audit program will include covered entities as well as their business associates and subcontractors.

In March 2013, the Department of Health and Human Services (HHS) issued a new rule to strengthen the privacy and security protections established under HIPAA for individual's health information maintained in electronic health records and other formats. In addition, the new rule will "modify the Enforcement Rules to implement statutory amendments under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act" or "the Act") to strengthen the privacy and security protection for individuals' health information; modify the rule for Breach Notification for Unsecured Protected Health Information" (45 CFR Parts 160 and 164).

ISO/IEC 27001 provides a comprehensive approach to the management of information system security. Its history goes back to 1995 when the original standard, BS 7799, was published.

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). These requirements describe the intended behavior of an ISMS, once it is fully operational. The standard is not a step-by-step guide on how to build or create an ISMS, but rather a set of risk-based specifications and controls. Organizations that meet these specifications can show that they have the security controls in place to address confidentiality, integrity, and availability.

ISO/IES 27001 Evolution



ISO/IEC 27002 is a guidance document that shares best practices for the implementation of ISO/IEC 27001. Together, these documents facilitate compliance to HIPAA/HITECH requirements.

ISO/IEC 27001 boils down to risk assessment, which HIPAA/HITECH heavily emphasizes. The standard defines controls in the following areas:

- Security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Examples of types of health information to be protected

As both HIPAA and ISO/IEC 27001 concentrate on the protection of information confidentiality, integrity and availability, there are several types of healthcare information that need this type of protection[1]. These include, but are not necessarily limited to:

a) personal health information[2]

b) pseudonymized data[3] derived from personal health information via some methodology for pseudonymous identification

c) statistical and research data, including anonymized data[4] derived from individual health information by removal of personally identifying data

d) clinical/medical knowledge not related to any specific subjects of care, including clinical decision support data (e.g. data on adverse drug reactions)

e) data on health professionals, staff and volunteers

f) information related to public health surveillance

g) audit trail data, produced by health information systems that contain personal health information, or pseudonymous data derived from personal health information, or that contain data about the actions of users with regard to personal health information;

h) system security data for health information systems, including access control data and other security related system configuration data for health information systems.

[1] ISO 27799:2008

[2] Personal health information (PHI), also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a healthcare professional to identify an individual and determine appropriate care.

[3] Pseudonymization takes the most identifying fields within a database and replaces them with one or more artificial identifiers, or pseudonyms. For example a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data retention and data sharing.

[4] "anonymized" data can be used to assess the efficacy of healthcare treatments and strengthen our capacity to provide patients with better, more efficient healthcare. But our health privacy laws today do not promote the use of anonymized data. Instead, our laws, in many cases, either permit or require the use of fully identifiable data (including patient names, addresses, phone numbers, etc.) for these functions, providing little incentive to remove identifiers from data before its use.

Comparison of the HIPAA Requirements to ISO/IEC 27001

The goal of this comparison is to answer the following questions:

1. If your current information systems meet the HIPAA Security Standards, do they also meet ISO/IEC 27001?
2. If your current information systems meet the ISO/IEC 27001, do they also meet/satisfy the HIPAA Security regulations?
3. What compliance strategy could be followed to be compliant with HIPAA and conform to ISO/IEC 27001?

This discussion can help a healthcare organization, required by law to meet the HIPAA standards as a covered entity, decide whether meeting the ISO standard is sufficient to meet the HIPAA requirements or is a complement to the HIPAA requirements. For an organization interested in meeting both standards, this would lead to an "Implement Once, Comply Many" strategy.

It is important to note that HIPAA is only concerned about the protection of PHI, while ISO/IEC 27001 is for the protection of any and all types of information. This comparison, however, looks at security controls without distinguishing the different types of confidential information. For simplicity sake and terms of this discussion, the table below describes the controls at a high-level.

Table 1 - HIPAA Appendix A to Subpart C of Part 164 - Security Standards: Matrix- ISO/IEC 27001 High Level Comparison Source: PivotPoint Security

HIPAA Security Standard	HIPAA Security Implementation Specification	ISO 27001:2013
Security Management Process 164.308(a)(1)	Risk Analysis	6.1.2 Information security risk assessment 8.2 Information security risk assessment
	Risk Management	6.1.3 Information security risk treatment 8.3 Information security risk treatment
	Sanction Policy	A.7.2.3 Disciplinary process
	Information System Activity Review	A.12.4.1 Event logging A.12.4.3 Administrator and operator logs A.16.1.2 Reporting information security events A.16.1.3 Reporting security weaknesses
Assigned Security Responsibility 164.308(a)(2)		A. 6.1.1 Information security roles and responsibilities
Workforce Security 164.308(a)(3)	Authorization and/or Supervision	A.9.2.2 User access provisioning
	Workforce Clearance Procedure	A.9.2.5 Review of user access rights
	Termination Procedures	A.7.3.1 Termination or change of employment responsibilities A.9.2.6 Removal or adjustment of access rights
Information Access Management 164.308(a)(4)	Isolated Health Clearinghouse Functions	N/A
	Access Authorization	A.9.2.2 User access provisioning
	Access Establishment and Modification	A.9.2.2 User access provisioning
Security Awareness and Training 164.308(a)(5)	Security Reminders	A.12.6.1 Management of technical vulnerabilities
	Protection from Malicious Software	A.12.2.1 Controls against malware
	Log-in Monitoring	A.12.4.1 Event logging
	Password Management	A.9.4.3 Password management system
Security Incident Procedures 164.308(a)(6)	Response and Reporting	A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information security events A.16.1.3 Reporting security weaknesses A.16.1.4 Assessment of and decision on information security events A.16.1.5 Response to information security incidents

HIPAA Security Standard	HIPAA Security Implementation Specification	ISO 27001:2013
Contingency Plan 164.308(a)(7)	Data Backup Plan	A.12.3.1 Information backup
	Disaster Recovery Plan	A.17.1.1 Planning information security continuity A.17.1.2 Implementing information security continuity
	Emergency Mode Operation Plan	A.17.1.1 Planning information security continuity A.17.1.2 Implementing information security continuity
	Testing and Revision Procedures	A.17.1.3 Verify, review and evaluate information security continuity
	Applications and Data Criticality Analysis	14.1.1 Information security requirements analysis and specification A.17.1.1 Planning information security continuity
Evaluation 164.308(a)(8)		A.18.2.3 Technical compliance checking
Business Associate Contracts and Other Arrangements 164.308(b)(1)	Written contract or other arrangement	A.15.1.2 Addressing security within supplier agreements
Facility Access Controls 164.310(a)(1)	Contingency Operations	A.17.2.1 Availability of information processing facilities
	Facility Security Plan	A.11.1.3 Securing offices, rooms and facilities A.11.1.4 Protecting against external and environmental threats
	Access Control and Validation Procedures	A.11.1.1 Physical security perimeter A.11.1.2 Physical entry controls
	Maintenance Records	A.11.2.4 Equipment maintenance
Workstation Use 164.310(b)		A.8.1.3 Acceptable use of assets A.11.1.5 Working in secure areas A. 12.1.1 Documented operating procedures
Workstation Security 164.310(c)		A.11.1.5 Working in secure areas
Device and Media Controls 164.310(d)(1)	Disposal	A.8.3.2 Disposal of media
	Media Reuse	A.8.3.1 Management of removable media
	Accountability	A.8.3.3 Physical media transfer A.11.2.6 Security of equipment and assets off-premises
	Data Backup and Storage	A.12.3.1 Information backup
Access Control 164.312(a)(1)	Unique User Identification	A.9.2.1 User registration and de-registration
	Emergency Access Procedure	A.9.2.2 User access provisioning
	Automatic Logoff	A.11.2.8 Unattended user equipment
	Encryption and Decryption	A. 10.1.1 Policy on the use of cryptographic controls
Audit Controls 164.312(b)		A.12.4.1 Event logging A.12.4.2 Protection of log information A.12.4.3 Administrator and operator logs
Integrity 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	A.18.1.3 Protection of records
Person or Entity Authentication 164.312(d)		A.9.2.4 Management of secret authentication information of users
Transmission Security 164.312(e)(1)	Integrity Controls	A.13.1.1 Network controls
	Encryption	A.10.1.1 Policy on the use of cryptographic controls

Analysis of Comparison

ISO/IEC 27001 vs HIPAA: The comparison shows that the ISO requirements include the HIPAA requirements. Not all ISO/IEC 27001 controls are listed as there are a substantial number of additional requirements that go beyond what HIPAA requires, making ISO/IEC 27001 more holistic in nature.

HIPAA vs ISO/IEC 27001: The HIPAA standard includes at least one requirement (Isolated Health Clearinghouse Functions) not specifically included in the ISO requirements. This is taken into consideration, even if there are substantially more ISO requirements. One should keep in mind, HIPAA is very specific and ISO/IEC 27001 is not prescriptive, when evaluating the following controls under ISO/IEC 27001:

A.6.1.2	**A.13.1.3**	**A.9.4.1**	**A.18.1.4**
A.15.1.2,	**A.13.2.2,**	**A.9.4.1**	**A.10.1.1**

It is important, however, to put things in perspective. ISO/IEC 27001 is more holistic in nature and may be used to assess the information security practices of a broader scope and include all the activities an organization conducts. HIPAA, on the other hand, is very specific to regulated healthcare activities, and the covered entity typically targets a very narrow and specific scope. HIPAA-covered entities must also comply with very specific privacy rules and the Electronic Data Interchange (EDI) Rule, but should be evaluated under the equipment and compliance sections of ISO/IEC 27001.

A practical action plan for using ISO/IEC 27001 to enhance and meet HIPAA Requirements - Implement Once, Comply Many

ISO/IEC 27001 provides a common sense approach to planning, implementing and maintaining an information security management system (ISMS).

The following steps are common to maintaining an ISMS and would apply to implementing additional controls into a current ISO/IEC 27001 management system.

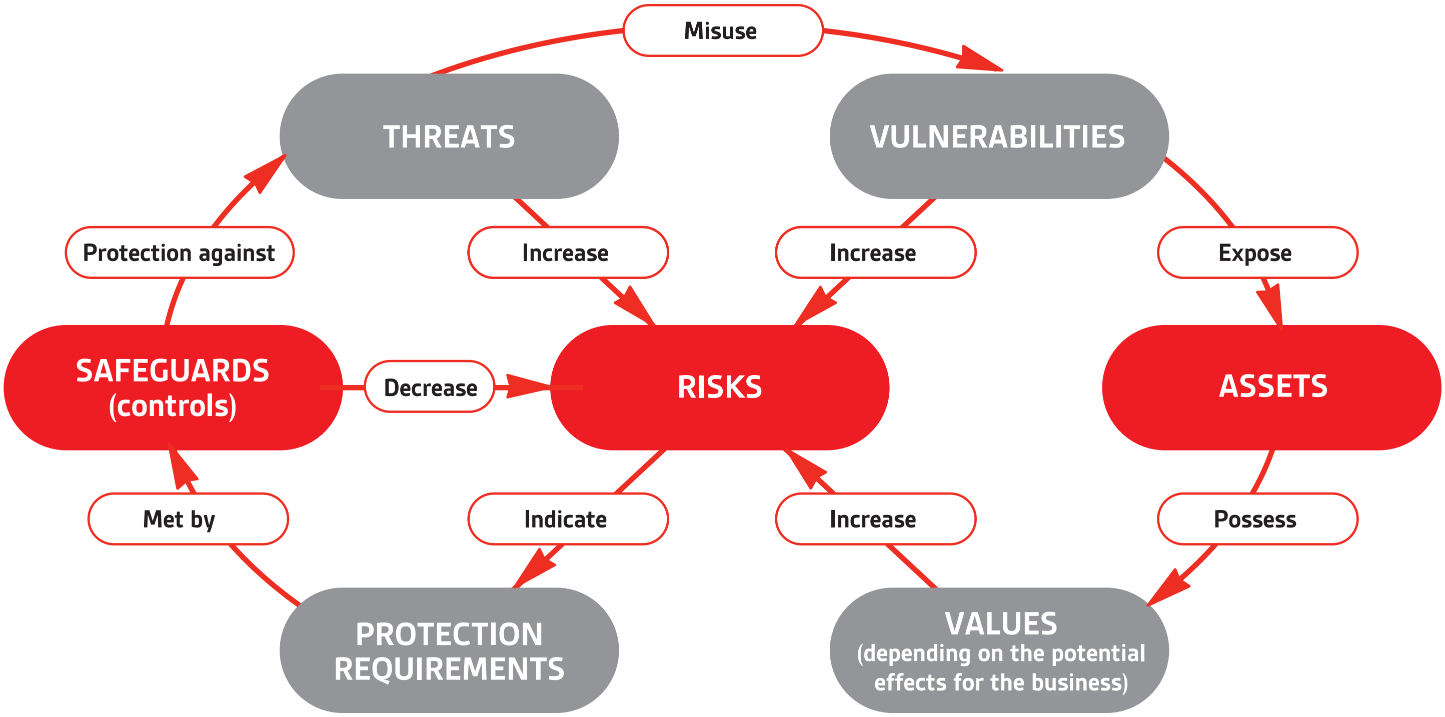
Analyze and Evaluate the Risks

Use your current risk methodology to apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system and identify risk owners. And Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, as well as impacts against the controls currently implemented.

Estimate the levels of risk and determine whether risks are acceptable or require treatment using the criteria for accepting risks that were previously established.

Assess the potential consequences that would result if the risks identified were to materialize;from possible security failures is identified and accounted for in existing controls.

Table 2 Simplified Risk Explanation - ISO/IEC 13335[5]



[5] Assets in terms of ISO/IEC 27001:2013 refers to Information Assets as opposed to IT Assets

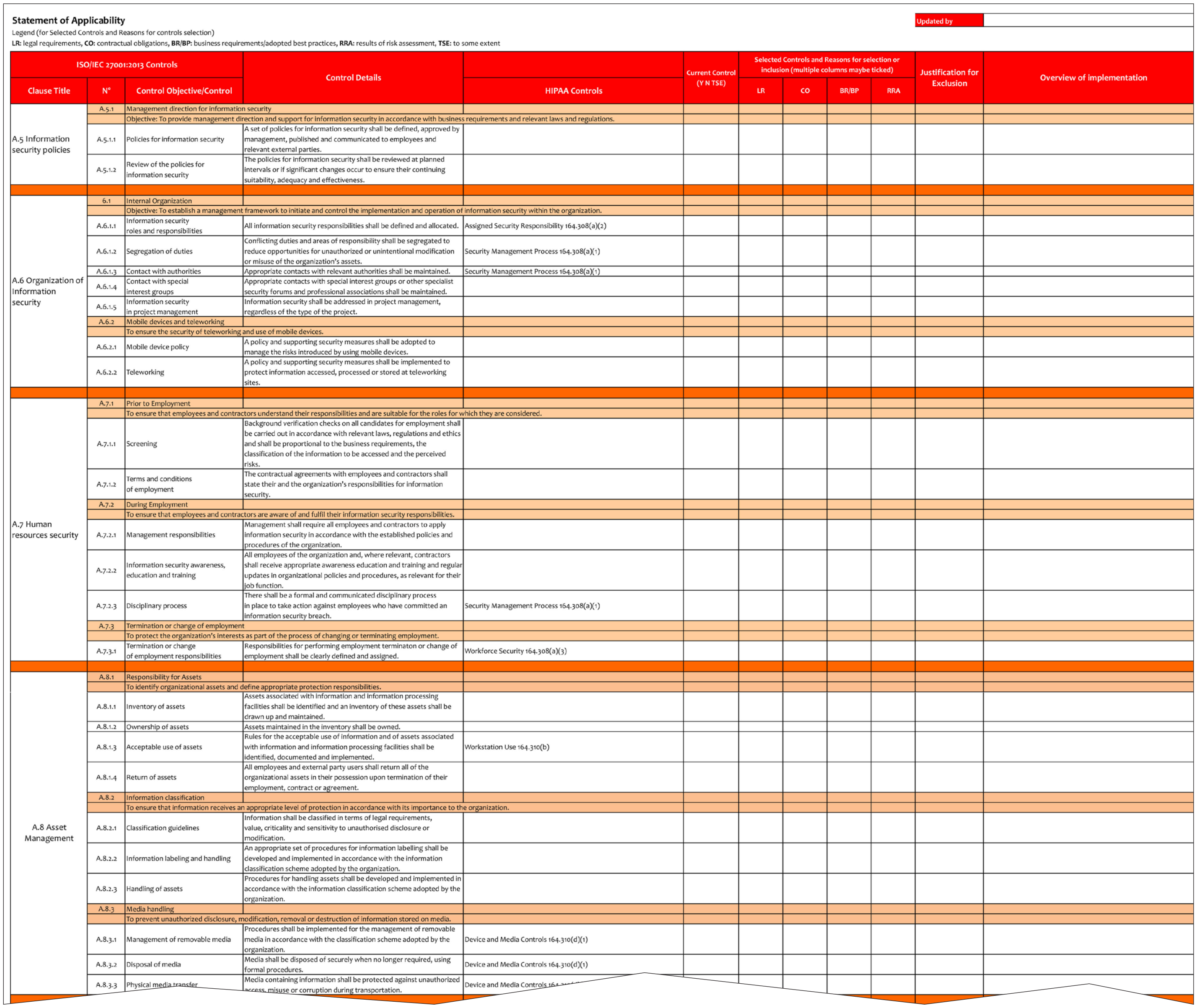
Add the controls to your Statement of Applicability (SOA)

The SOA[6] is a summary of reasons for selection and justification of inclusions of all controls and exclusions of controls from Annex A and must be supported by the risk analysis and evaluation and must fall within the scope of the ISMS. The specific applicable HIPAA security controls (see Table 1) are then simply added to the SOA, cross-mapping them to the corresponding ISO/IEC 27001 controls.

This mapping does a couple of things. First, it provides a quick reference to the HIPAA controls and the corresponding ISO/IEC 27001 controls. Second, because of all the additional requirements of ISO/IEC 27001 that address information security at the enterprise level including interrelationships, it shows that a more comprehensive standard of care has been implemented to include the more complex context[7] of the organization.

The HIPAA controls now become part of the enterprise-level ISMS showing not only due diligence and a high-level standard of care, but also consistency, organization and involvement by all stakeholders, including hands-on involvement by the organization's leadership.

Table 3 Sample SOA with Applicable HIPAA Controls



Statement of Applicability

Updated by

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO:** contractual obligations, **BR/BP:** business requirements/adopted best practices, **RRA:** results of risk assessment, **TSE:** to some extent

ISO/IEC 27001:2013 Controls			Control Details		Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification for Exclusion	Overview of implementation
Clause Title	N°	Control Objective/Control		HIPAA Controls		LR	CO	BR/BP	RRA		
A.5 Information security policies	A.5.1	Management direction for information security									
		Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.									
	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.								
	A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.								
A.6 Organization of Information security	6.1	Internal Organization									
		Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.									
	A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Assigned Security Responsibility 164.308(a)(2)							
	A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Security Management Process 164.308(a)(1)							
	A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Security Management Process 164.308(a)(1)							
	A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.								
	A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.								
	A.6.2	Mobile devices and teleworking									
		To ensure the security of teleworking and use of mobile devices.									
	A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.								
	A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.								
A.7 Human resources security	A.7.1	Prior to Employment									
		To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.									
	A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.								
	A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.								
	A.7.2	During Employment									
		To ensure that employees and contractors are aware of and fulfil their information security responsibilities.									
	A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.								
	A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.								
	A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Security Management Process 164.308(a)(1)							
	A.7.3	Termination or change of employment									
		To protect the organization's interests as part of the process of changing or terminating employment.									
	A.7.3.1	Termination or change of employment responsibilities	Responsibilities for performing employment terminaton or change of employment shall be clearly defined and assigned.	Workforce Security 164.308(a)(3)							
A.8 Asset Management	A.8.1	Responsibility for Assets									
		To identify organizational assets and define appropriate protection responsibilities.									
	A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.								
	A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.								
	A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Workstation Use 164.310(b)							
	A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.								
	A.8.2	Information classification									
		To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.									
	A.8.2.1	Classification guidelines	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.								
	A.8.2.2	Information labeling and handling	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.								
	A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.								
	A.8.3	Media handling									
		To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.									
	A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Device and Media Controls 164.310(d)(1)							
	A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Device and Media Controls 164.310(d)(1)							
	A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Device and Media Controls 164							

[6] The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

[7] The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

Conclusion

ISO/IEC 27001 has security controls for a number of areas not covered by HIPAA. This is not surprising, as the goal of HIPAA was to standardize just one kind of information, PHI, not all information. This is an important consideration, since many systems are now integrated. The potential risk and impact must be evaluated to determine if the PHI is being protected on all fronts and not treated as an island of information.

As both standards are risk-based, consider the following strategy to ensure your organization is compliant with both standards:

1. Conduct a risk assessment for those information systems under review, taking into account the context of the organization.
2. Ensure the scope matches the critical assets and processes.
3. Specify the ISO/IEC 27001 controls to be applied to each system.
4. Cross-reference the ISO controls to the HIPAA requirements.
5. Add any additional required HIPAA controls that may not be required by ISO, including the HIPAA organizational and documentation requirements.
6. Develop and implement policies and procedures applicable to the full set of selected ISO and HIPAA controls.
7. Perform a training needs analysis to ensure all stakeholders have been properly trained and are competent.
8. Consider software tools that may help reduce the tracking and administrative burden of managing an ISMS.
9. Perform internal audits, reviewing compliance with the full set of controls.
10. Put in place additional metrics to continuously monitor the relevant HIPAA requirements as part of the overall ISMS and continual improvement process.

Meeting the HIPAA Security Standards is a legal requirement for healthcare covered entities. The HIPAA Omnibus rule that went into effect September 23, 2014 makes it clear that business associates of covered entities and their subcontractors are now directly responsible for HIPAA compliance. It is also critical to point out that patient information could fall under multiple regulations, e.g. HIPAA (patient information), PCI-DSS (payment for care), PII (personal demographics including SSN) and Human Research Common Rule for privacy of research subjects. Meeting the ISO/IEC 27001 requirements demonstrates a complete approach to information security and that internationally recognized best practices are in use. This is becoming increasingly important, with the growing popularity of cloud computing and data crossing international boundaries. With ISO/IEC 27001, an organization can meet and exceed multiple regulatory requirements, while providing customers with the assurance of using meeting an international industry best practice for information security and standard of care.

BSI would like to express its appreciation to Kevin Hardcastle, CISO at Washington University, for his contribution and review of this whitepaper.

bsi.

To find out more, visit www.bsiamerica.com

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA

Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
Web: www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada

Tel: 1 800 862 6752
Fax: 1 416 620 9911
Email: Inquiry.canada@bsigroup.com
Web: www.bsigroup.ca
www.bsigroup.ca/fr