Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The HIPAA Final Security Standards and ISO/IEC 17799

Compliance with the HIPAA Final Security Standards is a regulatory requirement for healthcare organizations. ISO/IEC 17799 is an international information security standard. This paper compares these two standards to see whether if in complying with one of the standards, the other is also satisfied. The paper concludes that the HIPAA Final Security Standards has a small number of requirements not covered by ISO/IEC 17799, and that ISO/IEC 17799 has a number of controls not covered by the HIPAA Security Standards. A det...

Copyright SANS Institute
Author Retains Full Rights

AD

The HIPAA Final Security Standards and ISO/IEC 17799

Sheldon Borkin

July 15, 2003
Practical Assignment for GIAC GSEC Certification
Version 1.4b, Option 1

Abstract

Compliance with the HIPAA Final Security Standards is a regulatory requirement for healthcare organizations. ISO/IEC 17799 is an international information security standard. This paper compares these two standards to see whether if in complying with one of the standards, the other is also satisfied.

The paper concludes that the HIPAA Final Security Standards has a small number of requirements not covered by ISO/IEC 17799, and that ISO/IEC 17799 has a number of controls not covered by the HIPAA Security Standards. A detailed analysis and cross-reference is provided along with an approach to compliance with both standards.

Background

HIPAA Final Security Standards. "HIPAA" is the Health Insurance Portability and Accountability Act of 1996 (CMS, "HIPAA Administrative Simplification - Background"). Title I of HIPAA relates to the portability of health insurance when workers change or lose jobs. Title II of HIPAA is the Administrative Simplification portion which aims to make the health care system more efficient through the increased use of standard electronic transactions (such as claims and insurance eligibility requests) for health care administration. Along with the regulations for the standardization of the transactions are regulations to protect the privacy and security of health care information.

To implement Administrative Simplification, the Department of Health and Human Services (HHS), through the Centers for Medicare and Medicaid Services (CMS) has (or will) defined four standards with various compliance dates for health care entities including providers (physicians and hospitals), payers (insurance companies and HMOs), and clearinghouses (bulk processors of transactions between providers and payers). The standards and major compliance dates are:

1. Privacy Standards - April 14, 2003
2. Transactions and Code Set Standards - October 16, 2003
3. Security Standards - April 20, 2005
4. Identifier Standards - not yet finalized

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Privacy Standards requires that "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" (CMS, "HIPAA Administrative Simplification - Privacy", Section 164.530 (c)(1)), but does not give any specifics as to what specific security controls must be in place.

In August 1998, a Proposed Security Rule was published (CMS, "HIPAA Administrative Simplification - Security; Proposed Rule"). After a period of comment-taking, and then a much longer period to draft a final document, the Final Security Rule (CMS, "HIPAA Administrative Simplification - Security; Final Rule") was published in February 2003. This is officially Subpart C of 45 CFR Part 164. The Final Security Rule is much more flexible than the Proposed Security Rule (Lamar) as it allows many of the requirements to be "addressable" which means that the exact type and level of controls to meet the requirement can be determined according to the required risk analysis. Those requirements which are not "addressable" are noted as "required".

The Final Security Rule requires safeguards for the protection of "electronic personal health information" (ePHI) in three general areas with specific implementation requirements in each area. The areas and numbers of implementation requirements are:

- Administrative Safeguards - 23 implementation requirements
- Physical Safeguards - 10 implementation requirements
- Technical Safeguards - 9 implementation requirements

Published in the Final Security Rule is a Response to Comments on the Proposed Rule which explains how each comment or group of comments submitted on the Proposed Rule relates to the Final Rule. These explanations are much longer than the Final Security Standards themselves and often give much better detail on how to interpret the standards, than the terse wording of the standards themselves.

ISO/IEC 17799 International Standard. The ISO/IEC 17799 International Standard (ISO/IEC) provides a comprehensive approach to the management of information system security. It is based on the British Standards Institution BS 7799 Part 1 (BSI).

ISO/IEC 17799 defines information security controls in the following ten areas:

- Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Similar to the HIPAA Security Standards' addressable requirements, the specific controls to be used from those listed in the standard are to be picked according to a risk assessment. Rather than the "required" controls of HIPAA's, there is in ISO/IEC 17799 an "Information security starting point" (ISO/IEC, p. x) with eight "essential" areas of control.

ISO does not provide certification against ISO/IEC 17799, but such certification is provided worldwide by BSI according to BS 7799 Part 2 which defines compliance and audit requirement including relationships to the ISO 9000 quality standards (BSI). An ISO/IEC 17799 audit checklist is available from The SANS Institute (Thiagarajan).

From an industry perspective, ISO/IEC 17799 has come under some criticism for being too general, but it is being adopted by many companies - and is the only international standard covering information security (Walsh). The ISO Technical Subcommittee JTC 1/SC 27 responsible for ISO/IEC 17799 has started the preparation work for doing a second edition, but no completion date is set (JTC 1/SC 27).

Comparison of the HIPAA Final Security Standards to ISO/IEC 17799

Following is a comparison of each of the HIPAA Security Standards requirements to those in the ISO/IEC 17799 International Standard. For conciseness, the HIPAA Security Standards is often referred to as just "HIPAA" and the ISO/IEC 17799 International Standard is often referred to as just "ISO" or "ISO/IEC 17799".

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

1. If information systems meet the HIPAA Security Standards, do they also meet ISO/IEC 17799?
2. If information systems meet the ISO/IEC 17799, do they also meet the HIPAA Security Standards?
3. What compliance strategy could be followed to be compliant with both standards?

The answers to these questions can help a healthcare organization required by law to meet the HIPAA standards decide whether meeting the ISO standards is a replacement or a complement to meeting the HIPAA standards. For an organization interested in meeting both standards, the answers to these questions can lead to a compliance and audit strategy.

The comparison considers only the HIPAA sections giving the administrative, physical and technical safeguards. Other sections relating to organizational requirements such as business associate contracts and documentation requirements such as retention period are not included in this comparison.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

While HIPAA is only about the protection of ePHI, ISO is for the protection of all types of information. This is an over-arching difference in focus, but this comparison looks at security controls without distinguishing the different types of confidential information.

In researching the intent of various HIPAA Final Security Standard requirements, reference was made to the Response to Comments on the Proposed Rule in the Final Rule (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III), as well as (Pricewaterhouse Coopers) and (Lamar).

The convention in the comparison is that in each section the first paragraph is a summary with short commentary on the HIPAA requirement. The second paragraph explains the relevant sections of ISO/IEC 17799 to the HIPAA requirement. Then a judgment is given as to how the two standards compare. The designations for the comparison are defined in Figure 1.

Designation	Meaning
ISO ~ HIPAA	For the topic of concern, the HIPAA and ISO requirements are approximately the same.
ISO > HIPAA	For the topic of concern, the ISO requirements include the HIPAA requirements as well as a substantial number of additional requirements.
HIPAA > ISO	For the topic of concern, the HIPAA standard includes at least one requirement not included in the ISO requirements. This designation may be used even if there are substantially more ISO requirements for the topic. The goal with this is to point out areas where the ISO standard does not fully contain the HIPAA standard.

Figure 1. - Designations for Comparison of Standards

For readability, ISO section numbers and titles are shown in italics while HIPAA section numbers and titles are shown in regular text.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

164.308 Administrative Safeguards

(a)(1)i Security Management

(a)(1)ii(A) Risk Analysis (required)

This requires "an accurate and thorough assessment" of the risks to the "confidentiality, integrity, and availability" of ePHI (electronic personal health information) (CMS, "HIPAA Administrative Simplification - Security; Final Rule", 164.308(a)(1)ii(A)).

ISO Introduction - What Is Information Security? defines information security as the protection of confidentiality, integrity, and availability of information. *ISO Introduction - Assessing Security Risks* describes the need for risk assessments to guide the selection of appropriate security controls.

ISO ~ HIPAA

(a)(1)ii(B) Risk Management (required)

This requires that appropriate security measures be put in place according to the risk analysis to protect ePHI. For the many addressable requirements, it is the risk analysis which is used to determine the level and type of control to be used.

ISO Introduction - Selecting Controls corresponds to the HIPAA concept of risk management.

ISO ~ HIPAA

(a)(1)ii(C) Sanction Policy (required)

This requires that sanctions be applied against employees who do not comply with the defined policies and procedures.

The ISO standard covers this requirement in *ISO 6.3.5 Disciplinary Process*. Other ISO sections address aspects of communicating and enforcing the sanctions: *ISO 6.1.4 Terms and Conditions of Employment*, *ISO 9.2.1 User Registration*, and *ISO 12.1.5 Misuse of Information Processing Facilities*.

ISO ~ HIPAA

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(a)(1)i(D) Information Security Activity Review (required)

This requires that items such as audit logs, access reports, and security incident reports be reviewed.

The primary ISO requirement for the logging and reviewing systems activity is *ISO 9.7.2 Monitoring System Use and Access* which gives significantly more detail than the HIPAA requirement such as assuring that the logging facility itself is secure. Other relevant sections are *ISO 4.1.2 Information Security Co-ordination* and *ISO 8.1.3 Incident Management Procedures* requiring the review of security incidents, and *ISO 8.4.3 Fault Logging* which also requires the review of error logs for the compromise of security controls.

ISO > HIPAA

(a)(2) Assigned Security Responsibility (required)

This requires that a designated security official have responsibility for the development of the policies and procedures to meet the HIPAA security standards. Note that this implies a single person has responsibility for both physical and computer security.

ISO 4.1.1 Management Information Security Forum focuses on a management forum, e.g. a management team, which emphasizes the shared responsibility for security across an organization, but it also says that "one manager should be responsible for all security related activities" (ISO/IEC, p. 3). *ISO 4.1.3 Allocation of Information Security Responsibilities* outlines several possibilities including having one person with overall information security responsibility. However, neither ISO section is as specific as the HIPAA requirement.

HIPAA > ISO

(a)(3)i Workforce Security

This section covers personnel management requirements relevant to the protection of ePHI. The generally relevant ISO section is *ISO 6 Personnel Security*.

(a)(3)ii(A) Authorization and/or Supervision (addressable)

The HIPAA Security Standard includes this "authorization" requirement as well as *Access Authorization* under *Information Access Management*. The requirement of this present section as part of *Workforce Security* seems to be a personnel management

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

requirement that workers who are to access ePHI or are to work in locations with potential access to ePHI specifically be authorized to do so. Consideration needs to be given to situations, such as with maintenance workers, where direct supervision in the facility might be appropriate.

ISO 6.1.1 Including Security in Job Responsibilities covers the notion that security responsibilities be associated with specific jobs, *ISO 6.1.2 Personnel Screening and Policy* covers the supervision of workers, and *ISO 7.1.4 Working in Secure Areas* addresses additional issues of supervision.

HIPAA ~ ISO

(a)(3)ii(B) Workforce Clearance Procedure (addressable)

This somewhat vaguely worded requirement relates to the process for deciding that a particular worker can be trusted with ePHI. In the Response to Comments on the Proposed Rule, it is stated that:

> "This feature was not intended to be interpreted as an absolute requirement for background checks. We retain the use of the term 'clearance,' however, because we believe that it more accurately conveys the screening process intended..." (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.E.3.b)

ISO 6.1.2 Personnel Screening and Policy outlines specifically the kinds of reference, vitae, and appropriate credit checks which should be required.

ISO > HIPAA

(a)(3)ii(C) Termination Procedures (addressable)

This requires that a procedure be established for terminating access to ePHI when employment is terminated.

The *ISO 6 Personnel Security* does not contain any discussion of a termination process. This seems to be a meaningful omission. *ISO 9.2.1 User Registration* does address the removal of access rights to information systems for workers who "have left the organization" (ISO/IEC, p. 34), but does not refer specifically to termination.

HIPAA > ISO

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(a)(4)i Information Access Management

The intent of this section is made more clear from the response to comments on the Proposed Rule:

> "Under the information access management standard, a covered entity must implement, if appropriate and reasonable to its situation, policies and procedures first to authorize a person to access electronic protected health information and then to actually establish such access. " (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.G.6.a)

The technical safeguards to enforce such access are covered in section (a)(1) of the Technical Safeguards section.

The generally relevant ISO section corresponding to Information Access Management is *ISO 9 Access Control*.

(a)(4)ii(A) Isolating Health Care Clearinghouse Functions (required)

This requirement is to protect ePHI in a clearinghouse from any larger organization of which it is a part. Per the responses to comments on the Proposed Rule, this very specific requirement is included to meet a specific reference (1173(d)(1)(B)) in the HIPAA legislation (CMS, "HIPAA Administrative Simplification - Background"). It really is an instance of the need to make sure that only authorized personnel access ePHI.

There is no specific corollary in the ISO standard.

HIPAA > ISO

(a)(4)ii(B) Access Authorization (addressable)

This requires the policies and procedures to authorize a worker's access to ePHI through a specific mechanism such as a workstation or program.

ISO 9.1.1 Access Control Policy requires the clear definition of access control rules applicable to individual users or groups of users. *ISO 9.2.1 User Registration* and *ISO 9.2.2 Privilege Management* include the steps to get appropriate authorization from system owners and from management.

HIPAA ~ ISO

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(a)(4)ii(C) Access Establishment and Modification (addressable)

This requires the policies and procedures to document, establish, review and modify an authorized worker's access to ePHI through a specific mechanism such as a workstation or program.

ISO 9.2.1 User Registration and *ISO 9.2.2 Privilege Management* include the steps to document, establish, review and modify access. A number of additional requirements are included such as giving users statements of their access rights and requiring users to sign statements acknowledging their conditions of access.

ISO > HIPAA

(a)(5)i Security Awareness and Training

This states that the standard is to "Implement a security awareness and training program for all members of its workforce (including management)" (CMS, "HIPAA Administrative Simplification - Security; Final Rule", 164.308(a)(5)(i)). However, the following four implementation requirements do not seem to specifically require such a training program, so the "Security Reminder" requirement has to be viewed as the overall placeholder for training - which is consistent with the Response to Comments on the Proposed Rule (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.E.5).

The other three items, such as "Protection from Malicious Software" don't seem on first reading to fit into the Security Awareness and Training category directly, unless interpreted as education about "Protection from Malicious Software". This interpretation is consistent with the Response to Comments on the Proposed Rule (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.E.5).

(a)(5)ii(A) Security Reminders (addressable)

This is the placeholder for periodic training

This requirement is covered by *ISO 6.2.1 Information Security Education and Training*.

HIPAA ~ ISO

(a)(5)ii(B) Protection from Malicious Software (addressable)

This is meant to be training in the use of virus protection software and on reporting when virus or other malicious software is detected.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This implies that such protection is present - or at least is covered as an addressable risk.

ISO 8.3 Protection Against Malicious Software is a comprehensive section of protection from malicious software and includes the training and reporting requirements. User reporting is also covered by *ISO 6.3.1 Reporting Security Incidents*.

HIPAA ~ ISO

(a)(5)ii(C) Log-in Monitoring (addressable)

This requirement is to train workers on how to monitor log-in attempt and reporting suspicious circumstances. This might include both system administrator training to monitor logs, and end-user training on ways to notice if somebody else had logged-in or attempted to log-in to their account.

ISO 9.7 Monitoring System User and Access has comprehensive requirements for systems monitoring from a systems administration perspective including unauthorized access, but there are no specific ISO requirements for training administrators or users with regards to log-in monitoring.

HIPAA > ISO

(a)(5)ii(D) Password Management (addressable)

This requires that workers be trained in password management including creating, changing and safeguarding the passwords. This could include both the administrator processes and the user processes.

The ISO standard covers the creation and distribution of passwords in *ISO 9.2.3 User Password Management*. *ISO 9.3.1 Password Use* covers user responsibilities including the need to provide users with the awareness of these responsibilities.

HIPAA ~ ISO

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(a)(6)i Security Incident Procedures

(a)(6)ii Response and Reporting (required)

This is a requirement to implement policies and procedures to identify, respond to, mitigate, and document security incidents and their outcomes.

Such processes are fully covered by the more inclusive *ISO 6.3 Responding to Security Incidents and Malfunctions.* This ISO section also includes the requirements to learn from incidents and the disciplinary process. *ISO 12.1.7 Collection of Evidence* gives some requirements for the proper collection of evidence from an incident.

ISO > HIPAA

(a)(7)i Contingency Plan

This requires the policies and procedures to deal with emergencies which damage systems containing ePHI.

Contingency planning is covered by *ISO 11 Business Continuity Management.*

(a)(7)ii(A) Data Backup Plan (required)

This requires retrievable copies of ePHI. No specific instructions are given as to the storage locations of back-ups.

ISO covers this requirement in *ISO 8.4.1 Information Back-up.* ISO provides additional information on items such as remote storage of back-ups, environmental protections for back-ups, and testing of the media and restoration process.

ISO > HIPAA

(a)(7)ii(B) Disaster Recovery Plan (required)

This requires the creation of a disaster recovery plan to restore loss of data.

ISO 11.1.3 Writing and Implementing Continuity Plans includes these requirements from the broader perspective of restoring business processes rather than just the data. *ISO 11.1.1 Business Continuity Management Process* and *ISO 11.1.4 Business*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Continuity Planning Framework gives significant additional detail as to the process for formulating and for what should be contained in the continuity plan.

ISO > HIPAA

(a)(7)ii(C) Emergency Mode Operation Plan (required)

This requires the continuation of business processes for the protection of ePHI. This acknowledges that there is a business process perspective to consider, but limits the regulatory requirements to the scope of protecting the ePHI and does not consider the issues of the business operation such as the customer commitments of the covered entity.

As described just above *ISO 11.1.1, 11.1.3 and ISO 11.1.4* have much more detailed descriptions of the contents required in a continuity plan, but the ISO description does not call out the particular need to make sure that security is maintained in the operations providing continuity.

HIPAA > ISO

(a)(7)ii(D) Testing and Revision Procedures (addressable)

This requires the testing and revision of contingency plans.

The testing of data back-up is covered in *ISO 8.4.1 Information Back-up* while the testing and update of the business continuity plan is covered in detail in *ISO 11.1.5 Testing, Maintaining, and Re-assessing Business Continuity Plans*. *ISO 11.1.1 Business Continuity Management Process* also requires this testing and updating.

ISO > HIPAA

(a)(7)ii(D) Applications and Data Criticality Analysis (addressable)

This requires that applications and data be assessed for criticality in supporting the contingency plan. This is the only specific mention of applications in the Contingency Plan section, does not limit the scope to ePHI, and does not actually say what to do with the analysis. It does not refer to the risk analysis required in the Administrative Safeguards, though it seems quite relevant.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ISO 11.1.2 Business Continuity and Impact Analysis derives requirements from a risk analysis and considers the entire business process, not just information systems.

ISO > HIPAA

(a)(8) Evaluation (required)

This requires the periodic evaluation of compliance with the policies and procedures supporting the HIPAA Security Standards.

ISO 12.2 Reviews of Security Policy and Technical Compliance specifies similar checking. It has some additional details such as a specific requirement for penetration testing.

ISO ~ HIPAA

(b)(1) Business Associate Contracts and Other Arrangements

This requires that the covered entity obtain assurances that ePHI entrusted to a third party receiving is protected. Note that it does not create an obligation on the covered entity to proactively audit the third party for compliance with the assurances.

Sections (2) and (3) deal with applicability and noncompliance with such assurances.

(4) Written Contract or Other Arrangement (required)

The assurances of protection from the third party must be documented in a written contract.

ISO 4.2.2 Security Requirements in Third Party Contracts and *ISO 4.3.1 Security in Outsourcing Contracts* require similar assurances. The two ISO sections consider the case of the covered entity receiving access to the covered entity systems and then the broader case in which the third party takes over responsibility for information processing.

ISO ~ HIPAA

164.310 Physical Safeguards

Physical Safeguards are covered by *ISO 7 Physical and Environmental Security*.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(a)(1) Facility Access Controls

This section describes the required controls on facilities containing ePHI or systems with access to ePHI.

(a)(2)(i) Contingency Operations (required)

This requires that contingency plans and related requirements (covered in (a)(7)i of the Administrative Safeguards) include facility access controls for those facilities used in the contingency operations.

Similarly to the shortcoming of ISO with respect to the lack of specific security items called out for the Emergency Mode Operation Plan, ISO does not specifically require facility access controls within the contingency plan.

HIPAA > ISO

(a)(2)(ii) Facility Security Plan (required)

This requires that there be a plan with policies and procedures to prevent "unauthorized physical access, tampering, and theft" (CMS, "HIPAA Administrative Simplification - Security; Final Rule", 164.310(a)(2)(ii)) from facilities containing or having access to ePHI.

ISO 7 Physical and Environmental Security has an extensive description of detailed controls and considerations for the securing of facilities including items such as facility siting, security perimeter definition, intruder detection systems, and the security of loading docks. But the ISO standard does not specifically require a physical security plan.

HIPAA > ISO

(a)(2)(iii) Access Control and Validation Procedures (addressable)

This requires that there be procedures to control and validate a person's access to a facility. This should take into account the person's role and whether they are a visitor. There is a specific mention that there be "control of access to software programs for testing and revision"(CMS, "HIPAA Administrative Simplification - Security; Final Rule", 164.310(a)(2)(iii)) - presumably for development and test activities which use ePHI as test data.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ISO 7.1.2 Physical Entry Controls covers access controls and validation procedures including details such as handling visitors and the wearing of identification.

ISO ~ HIPAA

(a)(2)(iv) Maintenance Records (addressable)

This requires policies and procedures to document repairs and modifications to facility components related to security such as walls, doors and locks.

The ISO standard has no specific requirement relating to physical security maintenance records.

HIPAA > ISO

(b) Workstation Use (required)

This requires policies and procedures on the proper use of workstations and on their proper physical attributes for the siting of workstations. Per the Response to Comments on the Proposed Rule, this is meant to include, for example, a requirement that users log off their workstation when leaving it (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.F.3). The requirement for creating policy on the physical attributes seems to overlap the following Workstation Security requirement.

ISO 9.3.2 Unattended User Equipment deals specifically with the requirements for securing unattended workstations while *ISO 7.2.1 Equipment Siting and Protection* deals with the siting of equipment both to prevent unnecessary access and to protect the equipment from environmental hazards.

ISO ~ HIPAA

(c) Workstation Security (required)

This is a requirement to limit physical access to workstations which access ePHI.

As mentioned just above, *ISO 7.2.1 Equipment Siting and Protection* deals with the siting of equipment to prevent unnecessary access.

ISO ~ HIPAA

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(d)(1) Device and Media Controls

This set of requirements governs the handling of hardware and electronic media containing ePHI including receipt and removal both external to the facility and within the facility. Per the Response to Comments on the Proposed Rule, this explicitly includes mass storage systems as well as removable media (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.F.5.b). The Response to Comments on the Proposed Rule also points out that several of the requirements are addressable as they may be considered too onerous for small physician offices (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.F.5.d).

These topics are covered in *ISO 8.6 Media Handling and Security*.

(a)(2)(i) Disposal (required)

This requires policies and procedures to address the proper disposal of hardware and electronic media containing ePHI.

Both *ISO 8.6.2 Disposal of Media* and *ISO 7.2.6 Secure Disposal or Re-Use of Equipment* outline the need for secure disposal and give several considerations.

ISO ~ HIPAA

(a)(2)(ii) Media Re-use (required)

This requires policies and procedures to address the proper re-use of hardware and electronic media containing ePHI.

ISO 7.2.6 Secure Disposal or Re-Use of Equipment outlines the need for procedures to be implemented on the re-use of storage devices and gives several considerations.

ISO ~ HIPAA

(a)(2)(iii) Accountability (addressable)

This requires the maintenance of records including the responsible party for the movements of hardware and electronic media.

ISO 5 Asset Classification and Control requires the definition of handling procedures according to an information classification scheme. This contrasts with the HIPAA Standard in which the only category of asset considered is ePHI. ISO *8.6.3 Media Handling and Security* includes controls for the handling of media including

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

keeping records of media removal and data recipients. *ISO 7.3.2 Removal of Property* speaks to the authorization for the removal of equipment and the logging of equipment movement as appropriate.

ISO ~ HIPAA

(a)(2)(iv) Data Backup and Storage (addressable)

This requires the backup of ePHI before moving equipment. This is addressable according to the risk assessment.

ISO 8.4.1 Information Back-up has a detailed description of the considerations for back-up procedures, but does not specifically point out considerations for back-ups before the movement of equipment.

HIPAA > ISO

164.312 Technical Safeguards

(a)(1) Access Control

This is the section specifying technical requirements for the control of access to ePHI. Only workers authorized to have access to ePHI should have access. Such controls are included in *ISO 9 Access Control*.

(a)(2)(i) Unique User Identification (required)

This requires a unique user identification to identify and track users accessing ePHI. "User" is defined as "a person or entity with authorized access"(CMS, "HIPAA Administrative Simplification - Security; Final Rule", 164.304). An entity, in this case, might be a system rather than a person, though it is not defined what would qualify as an "entity".

ISO 9.2.1 User Registration speaks to having unique user ids while *ISO 9.5.3 User Identification and Authorization* gives more details. As it allows for the use of group ids "in exceptional circumstances" (ISO/IEC, p. 41), it is less stringent than HIPAA. The ISO Standard appears to view only people as users and does not acknowledge, for example, other systems as users.

HIPAA > ISO

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(a)(2)(ii) Emergency Access Procedure (required)

This requires procedures for obtaining access to ePHI during an emergency. This is the information systems aspect of access control required by Administrative Safeguard (a)(7)ii(C) Emergency Mode Operation Plan. The corresponding physical safeguard for emergency operations is Physical Safeguard (a)(2)(i) Contingency Operations.

As with the administrative and physical safeguards, the ISO document does not explicitly require that the access security aspects of emergency operations be addressed by the contingency plan or technology.

HIPAA > ISO

(a)(2)(iii) Automatic Logoff (addressable)

This requires time-outs for sessions after a period of inactivity. The specific period is addressable per the risk assessment. The Response to Comments on the Proposed Rule makes clear that as an addressable requirement other means besides logoff could be used to obtain the same effect (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.G.1.b). For example, a password-protected screen-saver could be used to provide an equivalent control.

ISO 9.5.7 Terminal Time-Out requires the same controls.

ISO ~ HIPAA

(a)(2)(iv) Encryption and Decryption (addressable)

This is to allow the use of file encryption of "data at rest" per the Response to Comments (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.G.1.c) as a means of access control. Encryption during transmission is covered in (e) below. The choice to use encryption is according to the risk analysis.

ISO 10.3.2 Encryption covers the use of encryption to protect the confidentiality of data according to a risk assessment. The remainder of *ISO 10.3 Cryptographic Controls* has significant additional guidance as to cryptographic policy and key management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ISO > HIPAA

(b) Audit Controls (required)

This requires the technology and procedures to record and examine information system activity. The level of auditing required is based upon the risk analysis. There is no specific requirement that every access to ePHI is recorded.

ISO 9.7 Monitoring System Use and Access has detailed explanations of controls for logging and reviewing events. The focus in the ISO standard is on exception situations.

ISO > HIPAA

(c)(1) Integrity

(c)(2) Mechanism to Authenticate Electronic Protected Health Information (addressable)

This requirement is to assure that ePHI is not altered or destroyed in an unauthorized manner. The Response to Comments on the Proposed Rule mentions several approaches to support this including check sums, error-correcting memory and digital signatures (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.G.3.a).

ISO 10.2.2 Checks and Controls describes a number of system-level and application controls to prevent the corruption of data while *ISO 10.3.3 Digital Signatures* describes the use of digital signatures. No specific mentions are made of low-level controls such as error-correction memory.

ISO ~ HIPAA

(d) Person or Entity Authentication (required)

This requires that verification is performed that a person or entity is the one claimed. In the Proposed Rule, specific technologies such as passwords, tokens and biometric identification were enumerated (CMS, "HIPAA Administrative Simplification - Security; Proposed Rule", II.3.e). In the Final Standards, no specific technology is proposed or required, though the addressable Password Management requirement in Security Awareness and Training acknowledges that importance of password systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ISO 9.5.3 User Identification and Authentication and *ISO 9.5.4 Password Management System* cover the topics of authentication and passwords while *ISO 9.4.3 User Authentication for External Connections* specifically addresses additional authentication controls for remote users.

ISO > HIPAA

(e)(1) Transmission Security

These requirements deal with the need to protect ePHI in transit over communication networks.

(e)(2)(i) Integrity Controls (addressable)

This requires that ePHI is not improperly modified during transmission.

ISO 10.2.3 Message Authentication describes hardware and software message authentication as a control to protect the integrity of transmitted information.

ISO ~ HIPAA

(e)(2)(ii) Encryption (addressable)

This is an addressable requirement for the use of encryption according to the risk analysis for data in transmission. The Proposed Rule was more prescriptive as to when encryption was needed such as requiring encryption on the Internet (CMS, "HIPAA Administrative Simplification - Security; Proposed Rule", II.4).

The Final Rule leaves even the decision of using encryption for the transmission of ePHI on the Internet to be based on the risk assessment though the Response to Comments on the Proposed Rule states that the use of encryption on the Internet is "encouraged" (CMS, "HIPAA Administrative Simplification - Security; Final Rule", III.G.5.a).

ISO 10.3.2 Encryption covers the use of encryption to protect the confidentiality of data according to a risk assessment. The remainder of *ISO 10.3 Cryptographic Controls* has significant additional guidance as to cryptographic policy and key management.

ISO > HIPAA

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 1, following the References section, summarizes the comparison above including the comparison designation and cross-references to ISO. Table 2 cross-references from the complete ISO table of contents to the related HIPAA sections.

Analysis of Comparison

For the 42 specific HIPAA Security Standards implementation requirements, Figure 2 shows how they compare to ISO/IEC 17799.

ISO ~ HIPAA	**19**
ISO > HIPAA	**12**
HIPAA > ISO	**11**

Figure 2 - Summary of Comparison of Standards

The ISO controls meet or exceed the HIPAA Standards for 31 (or 74%) of the implementation requirements. But given that the ISO standard is 71 pages vs. HIPAA's 5 pages, what is the composition of those HIPAA items which don't show up in ISO/IEC 17799? The eleven such items are shown in Figure 3 along with an explanation of the difference between HIPAA and ISO for that requirement.

Requirements of HIPAA Not Fully Present in ISO		
	Requirement	Explanation
1	Administrative: (a)(2) Assigned Security Responsibility (required)	HIPAA requires a single person responsible for both information and physical security.
2	Administrative: (a)(3)ii(C) Termination Procedures (addressable)	ISO has no mention of terminations anywhere in the document.
3	Administrative: (a)(4)ii(A) Isolating Health Care Clearinghouse Functions (required)	Unique requirement of the HIPAA legislation.
4	Administrative: (a)(5)ii(C) Log-in Monitoring (addressable)	ISO does not have a specific training requirement with respect to log-in monitoring.
5	Administrative: (a)(7)ii(C) Emergency Mode Operation Plan (required)	ISO does not specifically address security for contingency operations.
6	Physical: (a)(2)(i) Contingency Operations (required)	ISO does not specifically address physical security for contingency operations.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7	Physical: (a)(2)(ii) Facility Security Plan (required)	Documentation not required by ISO.
8	Physical: (a)(2)(iv) Maintenance Records (addressable)	Documentation not required by ISO.
9	Physical: (a)(2)(iv) Data Backup and Storage (addressable)	ISO does not specifically require data back-up before moving storage units.
10	Technical: (a)(2)(i) Unique User Identification (required)	ISO allows group user ids in some cases. Does not address entity authentication.
11	Technical: (a)(2)(ii) Emergency Access Procedure (required)	ISO does not specifically address access controls for contingency operations.

Figure 3 - HIPAA Requirements Not Fully Present in ISO

Item 1 from Figure 3 relates to a desire under HIPAA to identify a single individual responsible for all security for the protection of ePHI. This is not necessarily normal industry practice as responsibility is often divided between computer security and physical security.

Item 2 from Figure 3 seems to show a shortcoming of ISO/IEC 17799 in not explicitly addressing termination procedures.

Item 3 from Figure 3 is unique to the healthcare industry and would not be expected in ISO/IEC 17799.

Two items(4 and 9) require specific training and procedures which are valid controls to consider, but not necessarily standard practice.

From Figure 3, three of the eleven items (5, 6, and 11) relate to the fact that *ISO 11 Business Continuity* is completely focused on the resumption of operations without specific mention of maintaining security during the emergency operations. It might be "assumed" that such security is necessary, but on balance it seems to be a shortcoming of ISO/IEC 17799.

Two of the items (7 and 8) relate to additional physical security documentation requirement. While ISO is focused on information security rather than physical security, the fact that *ISO 7 Physical and Environmental Security* does not require a facility security plan is a shortcoming of ISO. The level of maintenance documentation required by HIPAA seems to be more stringent than most industry practices.

Item 10 from Figure 3 shows HIPAA as being even more stringent that ISO in its requirement for unique identification.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Additional ISO/IEC 17799 Controls Beyond HIPAA

Reference to Table 2 shows a large number of topics for which there is no HIPAA Security Standards cross-reference. Some of the major areas in which ISO/IEC 17799 has requirements for detailed controls beyond those of HIPAA are:

- Security in the systems development and maintenance process
- Network security
- Equipment security
- Management of security in outsourcing arrangements
- Asset classification policy (as HIPAA only distinguishes ePHI from non-ePHI)
- Operations security
- Mobile security and remote access

Reference to an audit checklist such as (Thiagarajan) also shows the full scope of ISO/IEC 17799.

Conclusion

The goal of this comparison and analysis was to answer three specific questions. The questions are restated below with their answers:

1. If information systems meet the HIPAA Security Standards, do they also meet ISO/IEC 17799?

   Answer: No. ISO/IEC 17799 has security controls for a number of areas not covered by HIPAA. As the goal of the HIPAA standards was to have standards for just one kind of information, ePHI, applicable to small physician offices as well as large healthcare organizations, it is not surprising that certain areas of control were left out of the standards.

2. If information systems meet ISO/IEC 17799, do they also meet the HIPAA Security Standards?

   Answer: No. The HIPAA Security Standards includes a small number of requirements which are either not included in ISO, or for which HIPAA has a more stringent requirement.

3. What compliance strategy could be followed to be compliant with both standards?

   Answer: As both standards require that controls be based on a risk assessment, the following strategy could be followed:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

a. Conduct a risk assessment for those information systems under review.
b. Specify the ISO/IEC 17799 controls to be applied to each system.
c. Cross reference the ISO controls to the HIPAA requirements (using Tables 1 and 2).
d. Add the additional HIPAA controls not required by ISO (per Figure 3), including the HIPAA organizational and documentation requirements not included in the previous comparison.
e. Develop and implement policies and procedures applicable to the full set of selected ISO and HIPAA controls.
f. Perform internal audits reviewing compliance with the full set of controls. External audits, as required, would likely focus on just the set of controls mandated by a specific standard, whether HIPAA or ISO.

Meeting the HIPAA Security Standards is a regulatory requirement for health care organizations. Meeting the ISO/IEC 17799 shows that internationally-recognized best practices are in use. By meeting both standards, an organization can meet and exceed the regulatory requirements while providing customers with the assurance of meeting an international industry standard for information security.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. British Standards Institution (BSI), "BS 7799", URL:http://www.bsi-global.com/Corporate/17799.xalter, (July 14, 2003).

2. Centers for Medicare and Medicaid Services (CMS), "HIPAA Administrative Simplification - Privacy", January 31, 2003, URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/default.asp, (July 14, 2003).

3. Centers for Medicare and Medicaid Services (CMS), "HIPAA Administrative Simplification - Security; Final Rule", March 21, 2003, URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp - finalrule, (July 14, 2003).

4. Centers for Medicare and Medicaid Services (CMS), "HIPAA Administrative Simplification - Background", January 31, 2003, URL:http://www.cms.hhs.gov/hipaa/hipaa2/general/background, (July 14, 2003).

5. Centers for Medicare and Medicaid Services (CMS), March 21, 2003, "HIPAA Administrative Simplification - Security; Proposed Rule", URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp, (July 14, 2003).

6. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC), International Standard ISO/IEC 17799, Information Technology - Code of practice for information security management (ISO/IEC 17799), First Edition, Geneva: ISO, December 1, 2000.

7. JTC 1/SC 27, "IT Security Techniques", July 1, 2003, URL:http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=143, (July 14, 2003).

8. Lamar, Marilyn, "Review of the New HIPAA Security Rule", March 14, 2003, URL:http://www.mahealthdata.org/mhdc/mhdc2.nsf/e16d87deedc61e9f86256a110020d8a6/b61b2aea63f0f96085256ce0000671bb/$FILE/SOF 20030314-Lamar.PPT, (July 14, 2003).

9. Pricewaterhouse Coopers, "Interpretation of the Final HIPAA Security Rule", April 15, 2003, URL: http://www.pwchealth.com, (July 14, 2003).

10. Thiagarajan, B.E., "AS/NZS 7799.2:2003, BS 7799.2:2002 Audit Check List", July 10, 2003, The SANS Institute, URL:http://www.sans.org/score/ISO_17799checklist.php, (July 14, 2003).

11. Walsh, Lawrence M., "Standard Practice", March 2002, URL:http://www.infosecuritymag.com/2002/mar/iso17799.shtml, (July 14, 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 1 - Cross-Reference from HIPAA Security Standard to ISO/IEC 17799 Standard

Implementation Requirements	HIPAA Security Safeguards	Comparison	Related ISO/IEC 17799 Controls
	164.308 Administrative Safeguards		
	(a)(1)i Security Management		
1	(a)(1)ii(A) Risk Analysis (required)	**ISO ~ HIPAA**	*ISO Introduction - Assessing Security Risks*
2	(a)(1)ii(B) Risk Management (required)	**ISO ~ HIPAA**	*ISO Introduction -Selecting Controls*
3	(a)(1)ii(C) Sanction Policy (required)	**ISO ~ HIPAA**	*ISO 6.3.5 Disciplinary Process* *ISO 6.1.4 Terms and Conditions of Employment* *ISO 9.2.1 User Registration* *ISO 12.1.5 Misuse of Information Processing Facilities.*
4	(a)(1)i(D) Information Security Activity Review (required)	**ISO > HIPAA**	*ISO 9.7.2 Monitoring System Use and Access* *ISO 4.1.2 Information Security Co-ordination* *ISO 8.1.3 Incident Management Procedures* *ISO 8.4.3 Fault Logging*
5	**(a)(2) Assigned Security Responsibility (required)**	**HIPAA > ISO**	*ISO 4.1.1 Management Information Security Forum* *ISO 4.1.3 Allocation of Information Security Responsibilities*
	(a)(3)i Workforce Security		

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6	(a)(3)ii(A) Authorization and/or Supervision (addressable)	**HIPAA ~ ISO**	*ISO 6.1.1 Including Security in Job Responsibilities* *ISO 6.1.2 Personnel Screening and Policy* *ISO 7.1.4 Working in Secure Areas*
7	(a)(3)ii(B) Workforce Clearance Procedure (addressable)	**ISO > HIPAA**	*ISO 6.1.2 Personnel Screening and Policy*
8	(a)(3)ii(C) Termination Procedures (addressable)	**HIPAA > ISO**	*ISO 9.2.1 User Registration*
	(a)(4)i Information Access Management		*ISO 9 Access Control*
9	(a)(4)ii(A) Isolating Health Care Clearinghouse Functions (required)	**HIPAA > ISO**	
10	(a)(4)ii(B) Access Authorization (addressable)	**HIPAA ~ ISO**	*ISO 9.1.1 Access Control Policy* *ISO 9.2.1 User Registration* *ISO 9.2.2 Privilege Management*
11	(a)(4)ii(C) Access Establishment and Modification (addressable)	**ISO > HIPAA**	*ISO 9.2.1 User Registration* *ISO 9.2.2 Privilege Management*
	(a)(5)i Security Awareness and Training		
12	(a)(5)ii(A) Security Reminders (addressable)	**HIPAA ~ ISO**	*ISO 6.2.1 Information Security Education and Training*
13	(a)(5)ii(B) Protection from Malicious Software (addressable)	**HIPAA ~ ISO**	*ISO 8.3 Protection Against Malicious Software* *ISO 6.3.1 Reporting Security Incidents*.
14	(a)(5)ii(C) Log-in Monitoring (addressable)	**HIPAA > ISO**	*ISO 9.7 Monitoring System User and Access*
15	(a)(5)ii(D) Password Management (addressable)	**HIPAA ~ ISO**	*ISO 9.2.3 User Password Management* *ISO 9.3.1 Password Use*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

	(a)(6)i Security Incident Procedures		
16	(a)(6)ii Response and Reporting (required)	**ISO > HIPAA**	*ISO 6.3 Responding to Security Incidents and Malfunctions* *ISO 12.1.7 Collection of Evidence*
	(a)(7)i Contingency Plan		*ISO 11 Business Continuity Management*
17	(a)(7)ii(A) Data Backup Plan (required)	**ISO > HIPAA**	*ISO 8.4.1 Information Back-up*
18	(a)(7)ii(B) Disaster Recovery Plan (required)	**ISO > HIPAA**	*ISO 11.1.3 Writing and Implementing Continuity Plans* *ISO 11.1.1 Business Continuity Management Process* *ISO 11.1.4 Business Continuity Planning Framework*
19	(a)(7)ii(C) Emergency Mode Operation Plan (required)	**HIPAA > ISO**	
20	(a)(7)ii(D) Testing and Revision Procedures (addressable)	**ISO > HIPAA**	*ISO 8.4.1 Information Back-up* *ISO 11.1.5 Testing, Maintaining, and Re-assessing Business Continuity Plans* *ISO 11.1.1 Business Continuity Management Process*
21	(a)(7)ii(D) Applications and Data Criticality Analysis (addressable)	**ISO > HIPAA**	*ISO 11.1.2 Business Continuity and Impact Analysis*
22	**(a)(8) Evaluation (required)**	**ISO ~ HIPAA**	*ISO 12.2 Reviews of Security Policy and Technical Compliance*
	(b)(1) Business Associate Contracts and Other Arrangements		

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

23	(b)(4) Written Contract or Other Arrangement (required)	**ISO ~ HIPAA**	*ISO 4.2.2 Security Requirements in Third Party Contracts* *ISO 4.3.1 Security in Outsourcing Contracts*
	164.310 Physical Safeguards		*ISO 7 Physical and Environmental Security*.
	(a)(1) Facility Access Controls		
1	(a)(2)(i) Contingency Operations (required)	**HIPAA > ISO**	
2	(a)(2)(ii) Facility Security Plan (required)	**HIPAA > ISO**	
3	(a)(2)(iii) Access Control and Validation Procedures (addressable)	**ISO ~ HIPAA**	*ISO 7.1.2 Physical Entry Controls*
4	(a)(2)(iv) Maintenance Records (addressable)	**HIPAA > ISO**	
5	**(b) Workstation Use (required)**	**ISO ~ HIPAA**	*ISO 9.3.2 Unattended User Equipment* *ISO 7.2.1 Equipment Siting and Protection*
6	**(c) Workstation Security (required)**	**ISO ~ HIPAA**	*ISO 7.2.1 Equipment Siting and Protection*
	(d)(1) Device and Media Controls		*ISO 8.6 Media Handling and Security*.
7	(a)(2)(i) Disposal (required)	**ISO ~ HIPAA**	*ISO 8.6.2 Disposal of Media* *ISO 7.2.6 Secure Disposal or Re-Use of Equipment*
8	(a)(2)(ii) Media Re-use (required)	**ISO ~ HIPAA**	*ISO 7.2.6 Secure Disposal or Re-Use of Equipment*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9	(a)(2)(iii) Accountability (addressable)	**ISO ~ HIPAA**	*ISO 5 Asset Classification and* Control *ISO 8.6.3 Media Handling and Security* *ISO 7.3.2 Removal of Property*
10	(a)(2)(iv) Data Backup and Storage (addressable)	**HIPAA > ISO**	*ISO 8.4.1 Information Back-up*
	164.312 Technical Safeguards		
	(a)(1) Access Control		*ISO 9 Access Control*.
1	(a)(2)(i) Unique User Identification (required)	**HIPAA > ISO**	*ISO 9.2.1 User Registration* *ISO 9.5.3 User Identification and Authorization*
2	(a)(2)(ii) Emergency Access Procedure (required)	**HIPAA > ISO**	
3	(a)(2)(iii) Automatic Logoff (addressable)	**ISO ~ HIPAA**	*ISO 9.5.7 Terminal Time-Out*
4	(a)(2)(iv) Encryption and Decryption (addressable)	**ISO > HIPAA**	*ISO 10.3.2 Encryption* *ISO 10.3 Cryptographic Controls*
5	**(b) Audit Controls (required)**	**ISO > HIPAA**	*ISO 9.7 Monitoring System Use and Access*
	(c)(1) Integrity		
6	(c)(2) Mechanism to Authenticate Electronic Protected Health Information (addressable)	**ISO ~ HIPAA**	*ISO 10.2.2 Checks and Controls* *ISO 10.3.3 Digital Signatures*
7	**(d) Person or Entity Authentication (required)**	**ISO > HIPAA**	*ISO 9.5.3 User Identification and Authentication* *ISO 9.5.4 Password Management System*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

			ISO 9.4.3 User Authentication for External Connections
	(e)(1) Transmission Security		
8	(e)(2)(i) Integrity Controls (addressable)	**ISO ~ HIPAA**	*ISO 10.2.3 Message Authentication*
9	(e)(2)(ii) Encryption (addressable)	**ISO > HIPAA**	*ISO 10.3.2 Encryption* *ISO 10.3 Cryptographic Controls*

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table 2 - Cross-Reference from ISO/IEC 17799 Standard to HIPAA Security Standard

ISO Security Standard	Related HIPAA Security Standard Safeguards
Introduction	
What is Information Security?	
Why Information Security is Needed	
How to Establish Security Requirements	
Assessing Security Risks	Risk Analysis
Selecting Controls	Risk Management
Information Security Starting Point	
Critical Success Factors	
Developing Your Own Guidelines	
1 Scope	
2 Terms and Definitions	
3 Security Policy	
3.1 Information Security Policy	
3.1.1 Information security policy document	
3.1.2 Review and Evaluation	
4. Organizational Security	
4.1 Information Security Infrastructure	
4.1.1 Management information security forum	Assigned Security Responsibility
4.1.2 Information security co-ordination	Information Security Activity Review
4.1.3 Allocation of information security responsibilities	Assigned Security Responsibility
4.1.4 Authorization process for	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

information processing facilities	
4.1.5 Specialist information security advise	
4.1.6 Co-operation between organizations	
4.1.7 Independent review of information security	
4.2 Security of Third Party Access	
4.2.1 Identification of risks from third party access	
4.2.2 Security requirements in third party contracts	Written Contract or Other Arrangement
4.3 Outsourcing	
4.3.1 Security requirements in outsourcing contracts	Written Contract or Other Arrangement
5 Asset Classification and Control	Accountability
5.1 Accountability for Assets	
5.1.1 Inventory of assets	
5.2 Information Classification	
5.2.1 Classification guidelines	
5.2.2 Information labeling and handling	
6 Personnel Security	
6.1 Security in Job Definition and Resourcing	
6.1.1 Including security in job responsibilities	Authorization and/or Supervision
6.1.2 Personnel screening and policy	Authorization and/or Supervision Workforce Clearance Procedure
6.1.3 Confidentiality agreements	
6.1.4 Terms and conditions of employment	Sanction Policy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6.2 User Training	
6.2.1 Information security education and training	Security Training
6.3 Responding to Security Incidents and Malfunctions	Response and Reporting
6.3.1 Reporting security incidents	Protection from Malicious Software
6.3.2 Reporting security weaknesses	
6.3.3 Reporting software malfunctions	
6.3.4 Learning from incidents	
6.3.5 Disciplinary process	Sanction Policy
7 Physical and Environmental Security	Physical Safeguards
7.1 Secure Areas	
7.1.1 Physical security perimeter	
7.1.2 Physical entry controls	Access Control and Validation Procedures
7.1.3 Securing offices, rooms and facilities	
7.1.4 Working in secure areas	Authorization and/or Supervision
7.1.5 Isolated delivery and loading areas	
7.2 Equipment Security	
7.2.1 Equipment siting and protection	Workstation Use Workstation Security
7.2.2 Power supplies	
7.2.3 Cabling security	
7.2.4 Equipment maintenance	
7.2.5 Security of equipment off-premises	
7.2.6 Secure disposal or re-use of equipment	Disposal Media Re-use
7.3 General Controls	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7.3.1 Clear desk and clear screen policy	
7.3.2 Removal of property	Accountability
8 Communications and Operations Management	
8.1 Operational Procedures and Responsibilities	
8.1.1 Documented operating procedures	
8.1.2 Operational change control	
8.1.3 Incident management procedures	Information Security Activity Review
8.1.4 Segregation of duties	
8.1.5 Separation of development and operational facilities	
8.1.6 External facilities management	
8.2 System Planning and Acceptance	
8.2.1 Capacity planning	
8.2.2 System acceptance	
8.3 Protection against malicious software	Protection Against Malicious Software
8.3.1 Controls against malicious software	
8.4 Housekeeping	
8.4.1 Information back-up	Data Backup Plan Testing and Revision Procedures
8.4.2 Operator logs	
8.4.3 Fault logging	Information Security Activity Review
8.5 Network Management	
8.5.1 Network controls	
8.6 Media Handling and Security	Device and Media Controls
8.6.1 Management of removable computer media	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

8.6.2 Disposal of media	Disposal
8.6.3 Information handling procedures	Accountability
8.6.4 Security of system documentation	
8.7 Exchanges of Information and Software	
8.7.1 Information and software exchange agreements	
8.7.2 Security of media in transit	
8.7.3 Electronic commerce security	
8.7.4 Security of electronic mail	
8.7.5 Security of electronic office systems	
8.7.6 Publicly available systems	
8.7.7 Other forms of information exchange	
9 Access Control	Information Access Management Access Control
9.1 Business Requirement for Access Control	
9.1.1 Access control policy	Access Authorization
9.2 User Access Management	
9.2.1 User registration	Sanction Policy Termination Procedures Access Authorization Access Establishment and Modification Unique User Identification
9.2.2 Privilege management	Access Authorization Access Establishment and Modification
9.2.3 User password management	Password Management
9.2.4 Review of user access rights	
9.3 User Responsibilities	
9.3.1 Password use	Password Management

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9.3.2 Unattended user equipment	Workstation Use
9.4 Network Access Control	
9.4.1 Policy on use of network services	
9.4.2 Enforced path	
9.4.3 User authentication for external connections	Person or Entity Authentication
9.4.4 Node authentication	
9.4.5 Remote diagnostic port protection	
9.4.6 Segregation in networks	
9.4.7 Network connection control	
9.4.8 Network routing control	
9.4.9 Security of network services	
9.5 Operating System Access Control	
9.5.1 Automatic terminal identification	
9.5.2 Terminal log-on procedures	
9.5.3 User identification and authentication	Unique User Identification Person or Entity Authentication
9.5.4 Password management system	Person or Entity Authentication
9.5.5 User of system utilities	
9.5.6 Duress alarm to safeguard users	
9.5.7 Terminal time-out	Automatic Logoff
9.5.8 Limitation of connection time	
9.6 Application Access Control	
9.6.1 Information access restriction	
9.6.2 Sensitive system isolation	
9.7 Monitoring System Access and Use	Audit Controls
9.7.1 Event logging	
9.7.2 Monitoring system use	Information Security Activity Review
9.7.3 Clock synchronization	
9.8 Mobile Computing and Teleworking	
9.8.1 Mobile computing	
9.8.2 Teleworking	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10 Systems Development and Maintenance	
10.1 Security Requirements of Systems	
10.1.1 Security requirements analysis and specification	
10.2 Security in Application Systems	
10.2.1 Input data validation	
10.2.2 Control of internal processing	Mechanism to Authenticate Electronic Protected Health Information
10.2.3 Message authentication	Integrity Controls
10.2.4 Output data validation	
10.3 Cryptographic Controls	Encryption and Decryption Encryption
10.3.1 Policy on the use of cryptographic controls	
10.3.2 Encryption	Encryption and Decryption Encryption
10.3.3 Digital signatures	Mechanism to Authenticate Electronic Protected Health Information
10.3.4 Non-repudiation services	
10.3.5 Key management	
10.4 Security of System Files	
10.4.1 Control of operational software	
10.4.2 Protection of system test data	
10.4.3 Access control to program source library	
10.5 Security in Development and Support Processes	
10.5.1 Change control procedures	
10.5.2 Technical review of operating system changes	
10.5.3 Restrictions on changes to software packages	
10.5.4 Covert channels and Trojan code	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10.5.5 Outsourced software development	
11 Business Continuity Management	Contingency Plan
11.1 Aspects of Business Continuity Management	Testing and Revision Procedures
11.1.1 Business continuity management process	Disaster Recover Plan
11.1.2 Business continuity and impact analysis	Applications and Data Criticality Analysis
11.1 3 Writing and implementing continuity plans	Disaster Recover Plan
11.1.4 Business continuity planning framework	Disaster Recover Plan
11.1.5 Testing, maintaining and re-assessing business continuity plans	Testing and Revision Procedures
12 Compliance	
12.1 Compliance with Legal Requirements	
12.1.1 Identification of applicable legislation	
12.1.2 Intellectual property rights (IPR)	
12.1.3 Safeguarding of organizational records	
12.1. 4 Data protection and privacy of personal information	
12.1.5 Prevention of misuse of information processing facilities	Sanction Policy
12.1.6 Regulation of cryptographic controls	
12.1.7 Collection of evidence	
12.2 Reviews of Security Policy and	Evaluation

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Technical Compliance	
12.2.1 Compliance with Security Policy	
12.2.2 Technical compliance checking	
12.3 System Audit Considerations	
12.3.1 System audit controls	
12.3.2 Protection of system audit tools	

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced