Achieving HIPAA Security Standards compliance by implementing an ISO/IEC 27000 series Information Security Management System (white paper)

v1 2005-12-04

COPYRIGHT

DISCLAIMER

the Zygma partnership LLC has applied its best endeavours in the preparation of this paper which it freely distributes for public edification but accepts no liability arising from its use or application by any other parties, howsoever arising. Errors may have arisen in the transposition of text from reference sources and the analysis, whilst undertaken diligently and in good faith, may contain oversights or omissions, and in any event is subjective and performed in a general context, without regard to the needs of any specific entity or party. Those who choose to act upon any statements or claims presented in this paper do so entirely at their own risk.

Zygma regrets that it has to state a disclaimer but, sadly, it's a pretty litigious society these days, so one does the risk analysis and works out one's risk treatment plans (ISO/IEC 27001:2005 §4.2.1 d), e), f), g)).

CONTENTS

1. Scope & purpose

This paper has been prepared to provide those organizations having an interest in compliance with the US Health Insurance Portability and Accountability Act (HIPAA - 1996, revised 2003) Security Standards[1], especially those in the business of handling 'electronically protected health information'[2], with an understanding of the inter-relationship between those Security Standards and the growing series of international standards addressing Information Security Management Systems (ISMS).

The paper shows how these ISMS standards can be applied by a business to demonstrate its compliance with the HIPAA whilst providing additional benefits, such as broader assurance across the whole (or a well-defined sub-unit) of an organization's information security management system and certified compliance of that system based upon an internationally-recognized scheme which will be acknowledged by business partners, investors, and customers.

The paper relates to the latest versions of the referred-to standards, as of the date of the paper's publication (see 'References').

[1] CFR Title 45 – Public Welfare, Subtitle A - Department of Health And Human Services, Part 164 "SECURITY AND PRIVACY", Subpart C, "Security Standards for the Protection of Electronic Protected Health Information".

[2] The term 'Electronic Protected Health Information' is a defined term within CFR 45 Part 164 Sub-part C § 160.103, deferring to CFR § 164.501 which defines Protected Health Information (PHI) as "individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information".

2. Background to referenced standards

2.1. Health Insurance Portability and Accountability Act

The US Health Insurance Portability and Accountability Act (HIPAA), passed in 1996, obligates healthcare organizations to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" (ref. CMS, "HIPAA Administrative Simplification - Privacy", § 164.530 (c)(1)).

However, the HIPAA did not provide guidance as to what measures and controls would be 'appropriate' and hence healthcare organizations have experienced difficulty in determining how they could show compliance. In 2003 a revision to the HIPAA led to the addition of a new Subpart, addressing security standards[1].

The Security Standards give substantial guidance to healthcare organizations, setting out clauses which require full compliance (the HIPAA does actually label these clauses as 'required') and other clauses where the subject organization (the 'covered entity', in HIPAA parlance) has to exercise judgment as to how, and the extent to which, they comply with them (labeled by the HIPAA as being 'addressable'). All the HIPAA Security Standards clauses are essentially mandatory (normative), although compliance with those which are addressable may in some cases be excluded if they can be shown to be inapplicable. Their inapplicability is for the subject organization to determine and defend.

The HIPAA sets out its Security Standards in § 164.306 to '318 inclusive: generally by stating a '*Standard*' followed by '*Implementation specifications*'. In some cases *Standards* are stated without related *Implementation specifications*. This paper assumes that stand-alone *Standards* clauses are also 'required' (the HIPAA makes no explicit statement in this regard).

Although the HIPAA sets out these standards clauses, it should be noted that it neither offers nor requires any specific information security framework within which they should be managed, nor a means for applying a commonly-accepted audit process which leads to certification of their compliance. Furthermore, it is appropriate that it does not address these issues, since it is a regulation. However, healthcare organizations which are subject to the Act (or indeed those which choose to comply in order to provide third-party services to organizations which are covered entities as defined by the Act) do need to address these issues and, for business efficiency reasons, should to do so in a fashion which integrates with their existing management systems with minimal additional load, commensurate with providing the comfort (for themselves as well as other parties) which comes from a high degree of assurance that they, as a covered entity, comply with the HIPAA. The ISO/IEC 27000 series of Information Security Management Systems (ISMS) standards provides them with such a means.

The full text of the HIPAA is available electronically from the Electronic Code of Federal Regulations beta test site[3]. That version of the text has been the basis for this analysis. In the remainder of this paper the abbreviation 'HIPAA' is used to refer to the Security Standards in particular.

2.2. ISO information security management system series

This series of standards is based upon existing and proven standards with additional standards presently being drafted by the International Standards Organization's (ISO/IEC). The actual development work is the responsibility of a specific sub-committee responsible for the development of Security Techniques, ISO/IEC JTC1 SC27. The ISMS-related standards will eventually be collected under the generic grouping ISO/IEC 27000.

At present there are two published standards in this family: ISO/IEC 27001:2005 "Technology – Security techniques –Information security management requirements", and ISO/IEC 17799:2005 "Information Technology – Security techniques – Code of practice for information security management" (which will eventually be re-issued as ISO/IEC 27002). Other standards are being drafted and will support the ISMS model as defined by 27001.

Both of these standards evolved in the UK and have now been published as British Standards for an entire decade. In that time they have been acknowledged around the world as being the leading edge in information security management practices, and honed through international feedback. Now they have gained international status through publication by the International Standards Organization (ISO) and the International Electro-technical Committee (IEC): 17799 in 2000, 27001 as recently as October 2005. Although these standards have been recognized in the USA by such bodies as Congress' Joint Economics Committee[4], a number of States and significant businesses, take-up has been generally weak because of its 'foreign' image. Today however the international standing of these standards is leading to them being more widely embraced in the USA. The ANSI-ASQ National Accreditation Board[5] (ANAB) is establishing an ISMS accreditation scheme which, for the first time, will put in place a US-based means of accrediting certification bodies who can

[3] see http://www.gpoaccess.gov/cfr/retrieve.html to search for this and other parts.

[4] in May 2002 the Joint Economic Committee of the US Congress reported on "SECURITY IN THE INFORMATION AGE" (http://www.fas.org/irp/congress/2002_rpt/jec-sec.pdf). In this report, under the heading 'VALIDATING COMPLIANCE - THE FUTURE OF INFORMATION PROTECTION' it is stated "*The defining standard for developing an information protection program around is ISO 17799, formerly British Standard 7799*". At the time of that report ISO/IEC 27001 had not been published. Were the JEC to revisit this subject today, one would expect the reference to 17799 to be replaced by reference to 27001.

[5] see http://www.anab.org/

perform ISMS audits. These accreditation services will be internationally harmonized, with common standards for the accreditation of ISMS certification bodies and for the qualification of trained ISMS auditors (which, already, many other nations have already established). Those certification bodies would then be able to offer truly US-based ISMS certification services. Their certifications will be recognized globally[6].

The full texts of ISO standards are available from standards bodies – suggested sources in the US are the American National Standards Institute[7] or BSI Americas[8], in the UK the British Standards Institute[9].

In the remainder of this paper, these standards will be referred to simply by their allocated common name or identification numbers, i.e. 27001, 17799.

2.3. HIPAA Security Standards / ISMS inter-relationship

27001 provides the basis of an information security management system, and 17799 provides a list of controls which organizations should take into consideration when defining their ISMS. A founding principle of these documents is that they provide a starting point from which an organization can develop its own specific ISMS, applying those controls which relate to its business objectives and the risks it has to deal with and, when necessary, adding additional specific controls which it requires. 27001 requires that adopters of that ISMS standard prepare a Statement of Applicability (SoA) which explains how each of the 133 controls in 17799 is responded to (including determinations that a control is not applicable). Furthermore, the standards form part of an overall certification scheme which enables ISMS owners to gain independent certification of their ISMS (against 27001).

The HIPAA Security Standards lack any such framework of controls and does not support, nor even suggest, any mechanism for demonstrating compliance with it. The Security Standards set out requirements which, to oversimplify a trifle, can be fulfilled through the application of suitable controls. One can therefore intuitively assert that by operating a suitably designed ISMS and having it formally certified, a healthcare organization could use its ISMS to ensure that HIPAA Security Standards required controls were selected from 17799, or added to those which 17799 offers, and properly implemented.

As ever, though, the devil is in the detail, and to fully understand that we need to perform a careful analysis of each HIPAA Security Standards clause against the ISMS standards, most particularly 17799. However, much of the demonstration of compliance comes not from having once identified appropriate controls but to be able to give assurance that one is effectively operating, managing, reviewing and improving them. An ISMS which can be certified against the management standard, i.e. 27001, delivers that assurance. The benefits of that assurance in HIPAA terms are further discussed in §5).

The following analysis will show that 17799 meets or exceeds some 92% of the HIPAA Security Standards requirements. Where 17799 is not sufficient in scope or rigour to meet the HIPAA Security Standards requirements the covered entity can introduce, within their ISMS, additional controls required to satisfy the remaining HIPAA requirements. Those additional controls should be added to the organization's SoA, which would form the basis

---

[6] it is also worth noting that 27001 includes informative Annexes which illustrate the correspondence between this standard and: OECD Guidelines for the security of Information Systems and Networks; ISO 9001:2000 "Quality management systems - Requirements", and ; ISO 14001:2004 "Environmental management systems - Requirements with guidance for use". These can be helpful in developing a single Internal Control System embracing many management disciplines.

[7] see http://webstore.ansi.org/ansidocstore

[8] see http://www.bsitraining.com/infosecurity_standards.asp

[9] see http://www.bsonline.bsi-global.com/

of a formal certification of that ISMS against 27001. That ISMS could also be used by the covered entity to manage not just its HIPAA compliance but the business-wide aspects of its information security.

An ISMS Certificate can be used to give confidence to business partners and clients, to Centers for Medicare & Medicaid Services (**CMS**), and potentially reduce insurance premiums and liability exposure (each through having demonstrated that accepted best practices are being applied to their HIPAA compliance and other aspects of managing the organization's business).

Furthermore, we have now, for the first time, an internationally-agreed framework for ISMS and it is understood that ANSI-ASQ National Accreditation Board[5] (ANAB) is establishing an ISMS accreditation scheme which will provide the USA with its own scheme, internationally recognized, rather than obliging US-based enterprises to seek certification of their ISMS using certifiers qualified off-shore.

3. Comparative assessment

In preparing this comparative mapping, each HIPAA Security Standards clause has been assessed against the controls identified in 17799, first for a match in the scope and intention of the clauses and then to determine the extent to which the 17799 clause would enable compliance with the HIPAA requirement. Wherever possible the principal level of comparison has been the HIPPA's '*Implementation specifications*' against 17799's "Implementation guidance". In some cases where there is a good match whole sections have also been mapped to one another, and some 17799 clauses (concerning legal compliance) have been mapped to the HIPAA as a whole entity. This latter point reflects the fact that HIPAA and 17799 are not just different in that they are a regulation versus a standard, but that they are complementary in terms of a covered entity's operations.

Each mapping gives an indication of whether it is a substantially equivalent match or whether the 17799 clause exceeds or falls short of being able to support a demonstration of compliance with the HIPAA requirement.

A business operating as a covered entity could also use this approach to map its other information security and audit requirements into a single information security management system, based upon the ISO ISMS model.

4. Findings and conclusions from the mapping

The HIPAA Security Standards have, in §164.306 to '316 inclusive, 41 specific clauses (ref. Appendix A to § 164 Subpart C). From these, this paper has extracted a total of 86 discrete requirements statements against which a 17799 control could potentially be mapped. Each HIPAA clause in this paper has been mapped to at least one 17799 clause. §8 shows this mapping based on the ordering of 17799; §10 shows the mapping based on the ordering of the HIPAA. The two matrices are hyper-linked so users can easily review the many-many relationships that this paper has revealed.

As already stated, 17799 has 133 specific controls. In the mapping in §8 there are 263 instances of HIPAA clauses mapping into 17799 controls. Of these there are only 24 mappings where the author finds there to be less than equivalence of scope and intention between the respective clauses. In all others it is judged that the means to show HIPAA compliance is present in the scope of the matching 17799 clause (subject to diligent ISMS-owner application of standards concerned).

If one assumes that clauses have equal weighting or importance (i.e. they are defined within the HIPAA and 17799 alike at a consistent level of granularity – this is a reasonable but not entirely reliable assumption) then one can deduce that 17799 meets or exceeds the HIPAA Security Standards requirements for 91% of the HIPAA's coverage. For the remaining 9% of the HIPAA coverage, supplemental text or additional controls have been introduced to better support

the HIPAA's requirements: the inclusion of additional controls to meet implementation-specific needs is entirely consistent with the ethos and guidance of 17799 (ref §9).

Without placing too much focus on the absolute percentage values given above, the findings show that one may state with confidence that ISO/IEC 17799:2005 is very substantially supportive of HIPAA compliance and that, when implemented within an ISMS in accordance with ISO/IEC 27001:2005, 17799 provides all the means to achieve that compliance in a framework which can also embrace the business' whole information security needs.

The matrix in §8 shows that some 17799 clauses are not directly mapped to any HIPAA clause. The key word here is 'directly': it is highly likely that in the implementation of an ISMS intended to fulfill the needs of a covered entity these clauses would be found to have value in the context of the overall management system, in order to support HIPAA compliance, but they are simply not directly related to its clauses.

5. How a certified ISMS benefits HIPAA Security Standards compliance

The HIPAA requires that organizations protect "*against **reasonably anticipated** threats or hazards to the security or integrity of information*" (§ 164.306 (a)(2)) and "*against **reasonably anticipated** uses and disclosures not permitted by privacy rules*" (§ 164.306 (a)(3)) and that the organization takes steps to ensure compliance by its workforce (§ 164.306 (a)(4)) - and perhaps by implication its suppliers and sub-contractors. Further, it accepts that covered entities may implement controls to mitigate harmful incidents "*to the extent practicable*" (§164.308 (a)(6)(ii)).

A covered entity will be better placed to argue that it has indeed taken reasonable measures to anticipate the risks towards electronic protected health information for which it has responsibility when it has:

a) taken control of its business processes and in particular its risk management;

b) adopted and implemented internally an internationally-recognized information security management standard (and complementary code of practice), and;

c) had its ISMS independently assessed and certified as compliant with the standard and with HIPAA Security Standards.

This would be particularly so in the event that some dispute or possibly a breach actually arises. The Department of Health and Human Services has itself indicated that, in the event of any reason to investigate a covered entity, it would look favourably upon those organizations that could demonstrate good-faith in their efforts to comply with the HIPAA. Operation of an effective ISMS based upon internationally-recognized best practices is surely such a good-faith measure.

Implementing an ISMS based upon 27001 and applying the controls listed in 17799 with additional controls as suggested in §9 is not only a practical consideration for any healthcare organization but a fundamental means to exercise management control over the business' whole information security responsibilities. By integrating its ISMS into its overall business practices, an organization can be better aware of the importance and value that information has for its survival and success.

Having a formal certification of its ISMS allows a business to give greater assurance to all parties interested: its customers, suppliers, investors, and by no means least its Board and workforce. It shows the organization's commitment, from the top down, to properly handling its obligations and responsibilities, managing effectively its business to ensure its long-term success, and being prepared to constantly review and improve its operations.

6. Practical application

For those organizations that want to implement an ISMS (either to address their HIPAA compliance issues, or for any other information security/internal control purpose) or to upgrade an existing ISMS, now is the time to start doing it. Both standards are now published in their 2005 versions and are available from standards institutions previously identified in this paper.

7. Mapping of ISO/IEC 17799:2005 to HIPAA Security Standards clauses

Before presenting an overview of the mapping matrices it is helpful to make some comments on how the mapping has been conducted and the results presented.

Firstly, this is not a comparison of two like references, i.e. documents having the same scope and intent in their usage. The HIPAA is a regulatory statement of what certain organizations (covered entities, to use its parlance) in a specific market sector must do in order to remain compliant with those sector-specific regulations; 17799 is an international standard which provides a code of practice, expressed as a set of controls having generic application, that application depending upon the scoping and requirements of an over-riding policy and business goals. Thus at a simplistic level, this is a comparison between a specific and a generic document; between a regulation (compliance with which is a legal obligation) and a standard (compliance with which is the exercise of choice). An inspection of the HIPAA Security Standards and 17799 will show that the former has a set of clauses which state how that document is to be interpreted, which entities are subject to it and what the subject entities are required to do – how they then do that to achieve compliance is for them to resolve, and possibly have to justify at a later date. 17799 sets out controls which have a significant level of explanation, tutorial and justification, whilst leaving it to the user of the standard to decide the extent to which they will implement those controls. Furthermore, it is worth noting that 17799 requires a system to implement its recommendations: the HIPAA Security Standards effectively require that such a system be in place, and hence 17799 alone is not enough. The relationship between 17799 and 27001 has already been explained, and the mapping has identified instances where the Security Standards are really looking for the system over and above a control *per se*.

For the reasons above, the mapping has been conducted with a 'comparative' judgment as to how the implementation of an ISMS based upon the controls in 17799, having regard to the language and description of those controls, would enable a covered entity to demonstrate that its HIPAA obligations were being adequately fulfilled – at least in terms of its compliance with the 'Security Standards'. This has led to considering, for each match, whether "*the 17799 controls are scoped and written in a way which matches the requirements set out in the HIPAA language, or otherwise do they have either insufficient descriptiveness and/or scope, or are they so extensive as to be significantly more helpful to an implementer?*" That this is to some degree a subjective process is recognized – but then so is information security!

Each source document employs structured headings and levels of abstraction and these have been matched as best can be.

The performance of the mapping has been performed in four principle steps. A first parse took each HIPAA clause and compared it against 17799 clauses, identifying those where the scope and/or intention were the same. A comparative determination was made, as discussed above. This identified an initial mapping that included HIPAA clauses for which there was no matching 17799 clause.

A second parse then reviewed all 17799 clauses for which no match had been initially identified, and a review of the HIPAA performed to see whether the 17799 topic was in fact addressed by the HIPAA, by a comparison of the concepts being described. Again, a comparative determination was made where additional matches were found. All HIPAA clauses were by then matched to at least one 17799 clause,

but not vice-versa. Those still un-mapped 17799 clauses were finally reviewed, and in most cases the lack of a mapping was justified on the basis of 'no direct relationship'. As already noted, the fact that there is no mapping is not a suggestion that that clause would have no place in an ISMS implemented by a covered entity – only that it would have an indirect relationship to the specific HIPAA clauses.

Finally, where the scope of a 17799 clause has significant shortcomings or does not fully address the HIPAA requirements, this is noted and a separate Extended Controls Set[10] (ECS) has been created to accommodate those shortcomings. Those additional controls should be added to the organization's SoA, which would form the basis of a formal certification of that ISMS against 27001. Thus, this paper creates the additional controls necessary to establish an ISMS which has the required focus to fully-address the HIPAA Security Standards.

(Where the subject organization's special needs cover differing topic areas (e.g. perhaps SOX, etc.) and there is a need for supplementary ISMS controls, a separate ECS should be developed for each area, modeled on the HIPAA example given in this paper).

In matching clauses between the two sources, the greatest level of specificity has been sought. By its nature, information security is a complex web of inter-relationships. The effect of an information security policy should have ramifications throughout an organization's procedures and processes, as there will be a relationship between staff training and awareness, and disciplinary procedures: staff cannot reasonably be expected to comply with rules and procedures with which they have not been made familiar, and so on. Thus there are numerous one-many and many-one relationships.

The matrix in §8 replicates the clauses of 17799 (column 1) and against them matches those HIPAA Security Standard clauses which the 17799 control would fulfill (col. 2), with a determination of the comparative coverage or strength of requirement between 17799 and the HIPAA requirements (col. 3). Additional commentary (col. 4) discusses how the referenced 1799 clauses compare or makes other pertinent observations and where a supplementary control is defined in the HIPAA Extended Controls Set, that too is cross-referenced.

The column addressing 'Comparative coverage' uses the following symbology to indicate ratings:

- □ □ □ □ 17799's controls have ***significant shortcomings*** in their ability to address the scope of HIPAA's requirements;
- ■ □ □ □ 17799's controls ***do not fully address*** the scope of HIPAA's requirements;
- ■ ■ □ □ 17799's controls are ***equivalent*** in scope to HIPAA's requirements (note – 'equivalent' does not necessarily mean 'equal to' or 'the same as');
- ■ ■ ■ □ 17799 provides ***additional guidance*** in its controls which would assist demonstrating HIPAA compliance;
- ■ ■ ■ ■ 17799 provides ***substantial additional guidance*** in its controls which would significantly assist demonstrating HIPAA compliance.

In §9, a second matrix gives fourteen new controls, the HIPAA Extended Control Set (ECS), supplementing those 17799 controls which fall short of supporting a demonstration of HIPAA compliance The additional controls are defined in the style of, and related to, 17799, and also in the form of a 27001 Statement of Applicability (SoA), fully inter-linked. In practice, a covered-entity should use those

[10] 'Extended Control Set' is a term created by Zygma to refer to a defined set of additional controls used by an organization to supplement the ISMS standard controls and extend the scope of its ISMS to suit its specific business environment and needs. The ECS is used to extend the scope of the SoA.

controls to extend their own Statement of Applicability.

In §10, a third matrix presents a complementary look-up between HIPAA Security Standards clauses and the matching 17799/HIPAA ECS clauses. The entries between all three matrices are dynamically linked so that users can readily make cross-reference between all clauses of one standard which reference the other, and vice-versa, and with the HIPAA ECS.

The HIPAA Security Standards clauses are categorized as being either 'required' or 'addressable'; this is indicated in the following matrices by '[R]' or '[A]' respectively.

Finally, in §11, there are suggestions as to how these measures can be practically implemented in an ISMS.

This white-paper is intended to explain the rationale and findings of Zygma's study into how an ISMS can satisfy the need for HIPAA compliance. The full text of this paper can be purchased, by contacting Zygma by email (Enquiries@Zygma.biz) or telephone +1 714 965 99 42. The full paper consists of some fifty-five pages of detailed mapping which would be invaluable to any orgamization wishing to ensure that its information security protection plans did indeed provide for HIPAA Security Standards compliance. The full paper is provided as a Word file which allows users full freedom to apply the findings in their preferred way. What follows are snap shots to illustrate the depth and substance provided in those mappings and the guidance for implementation.

8. HIPAA Security Standards clauses against 17799

17799:2005 control	Matching HIPAA SS implementation specification(s)	Comparative coverage: 17799 cf. HIPAA	Commentary / Observations
			v) 'Control' is noted in 17799 as being a synonym for 'Safeguard', which is used (but not explicitly defined) within the HIPAA definitions.¶ § 164.103 definitions are not InfoSec-related.
3. STRUCTURE OF [the 17799] STANDARD	No equivalent stipulation		No equivalent whole section in the HIPAA. No conformity issue – subordinate 17799 clauses not listed.
4 RISK ASSESSMENT AND TREATMENT			HIPAA addresses the need to assess risk, but through requirements rather than as a topic. See subordinate 17799 clauses.
4.1 ASSESSING SECURITY RISKS	§ 164.306 (a)(2), (3) *General requirements* – protect against	■ ■ ■ □	Risk assessment should determine which risks it is reasonable to consider and what controls are adequate to mitigate against that risk (NB – HIPAA says 'protect', which may be considered more certain than mitigation, but §164.306(b) admits that flexibility must be applied, and words such as 'appropriate' and 'reasonable' are used.
	§ 164.306 (b) *Flexibility of Approach* (including all subordinate clauses)	■ ■ ■ □	Risk assessment should account for factors recognized by the referenced HIPAA clause, to select appropriate controls.
	§ 164.308 (a)(1)(ii)(A) *Risk analysis* [R]	■ ■ ■ □	
	§ 164.306 (d)(2) *Implementation specifications* – must implement 'required'	■ ■ □ □	Implicit in a policy statement to comply with HIPAA and associated risk assessment.
	§ 164.306 (d)(3)(i) *Implementation specifications* – must assess 'addressable'	■ ■ □ □	Implicit in a HIPAA risk assessment.
	§ 164.306 (d)(3)(ii)(A), (B) *Implementation specifications*	■ ■ □ □	Implicit in a HIPAA risk assessment. Note - ISO/IEC 27001's requirement for a Statement of Applicability would provide an ideal

9. HIPAA Extended Controls Set

In this section, the full paper sets out specific controls as an extension to those within the ISO/IEC 27001:2005 Statement of Applicability (SoA) for those HIPAA Security Standards clauses for which 17799 mappings in the preceding matrix were rated as having significant shortcomings or not fully addressing the Security Standards' needs. These controls and their related implementation guidance reflect the form and structure of the 27000 series, and the ethos which it promotes.

The matrix is divided into a number of sections, each one addressing a specific HIPAA Security Standards Section.

Collectively, columns 1, 2 and 3 of the matrix provide normative material which matches the 'Control Objectives' of 27001 Annex A: column 1 gives a reference for identification purposes; column two gives the Control objective and column 3 gives the control.

Column 4 of the matrix gives informative implementation guidance in the form and style of 17799 (and if the text in column 3 is 'de-rated' to be informative, i.e. 'shall' amended to 'should', then column 3 would mimic the 17799 representation of the control). The guidance given is generally briefer than that in 17799 for two reasons: firstly, the guidance is given in the specific context of a HIPAA Security Standards clause, rather than the generic approach of 17799; secondly, the specific HIPAA Security Standards requirement is often addressed by making more specific the scope of a sub-part of a 17799 clause, rather than the whole clause.

Finally, column 5 references the relevant HIPAA Security Standards clause and the 17799 clause on which the new control is modeled. Each of these references is hyper-linked to the other matrices.

The following figure illustrates the general form of this matrix, which provides a total of fourteen HIPAA Security Standards-specific extended controls.

HIPAA ECS control ref	Control objective	Control	Implementation guidance	Related HIPAA & 17799 clauses
Hecs.308	***Administrative safeguards***			
Hecs.308.1	Access management	User's access rights shall be established and modified according to a formal access control policy.	Multi-user systems that require protection against unauthorized access should have the allocation of user's access rights controlled according to formal access authorization policies. The following steps should be addressed: a) policies and procedures must be established to manage the establishment, documentation, review, modification and termination of all access authorizations. b) each user's access privileges associated with each workstation, transaction, program, or process should be identified; c) privileges should be allocated to users on a need-to-use	§ 164.308 (a)(4)(ii)(C) *Access establishment and modification* [A] *11.2.2 Privilege management*

10. Linked reverse mapping (HIPAA to 17799 & ECS)

In the full paper this section gives a reverse-mapping, complementing the detail mappings in the section giving HIPAA Security Standards clauses against 17799. Each HIPAA Security Standards clause is related to all ISMS controls which bear upon it, including the extended controls, where these apply.

The matrix shows that each HIPAA clause has at least one matching 17799 clause. Where the 17799 coverage is deemed insufficient, a further reference to the applicable HIPAA Extended Control is given.

HIPAA requirement	Matching 17799 implementation guidance	Commentary / Observations
	11.3.1 *Password use* 11.3.2 *Unattended user equipment* 11.3.3 *Clear desk and clear screen policy*	
§ 164.310 (c) *Workstation security* [R]	7.1.1 *Inventory of assets* 7.1.2 *Ownership of assets* 7.1.3 *Acceptable use of assets*	
§ 164.310 (d)(1) *Device and media controls*	10.7.1 *Management of removable media*	
§ 164.310 (d)(2)(i) *Disposal* [R]	9.2.6 *Secure Disposal or Re-Use of Equipment* 10.7.2 *Disposal of Media*	
§ 164.310 (d)(2)(ii) *Media re-use* [R]	9.2.6 *Secure Disposal or Re-Use of Equipment*	See Hecs.310.3.
§ 164.310 (d)(2)(iii) *Accountability* [A]	7.1.1 *Inventory of assets* 7.1.2 *Ownership of assets* 9.2.7 *Removal of Property* 10.7.1 *Management of removable media* 10.7.3 *Information handling procedures*	
§ 164.310 (d)(2)(iv) *Data back-up and storage* [A]	10.5.1 *Information Back-up*	See Hecs.310.4.

11. Implementing an ISMS to show HIPAA Security Standards compliance

Covered entities wishing to implement an ISMS addressing HIPAA Security Standards-compliance, either exclusively or as a part of an organization-wide ISMS, can use the matrices within this report to supplement their Statement of Applicability (SoA), which is an essential document required when implementing an ISMS.

The SoA is given in Annex A of 27001. It states a 'Control objective' (as a title) and then a normative 'Control'. These control objectives and controls are derived directly from 17799, §5 - §15 inclusive, where extensive informative guidance is given.

For each control an organization should determine the applicability of the control and determine how it will respond to it, taking into account the applicable 17799 guidance. Not all controls will apply to all organizations, and not all organizations will find the controls there listed to be sufficient. Such is the case when seeking to readily show HIPAA Security Standards compliance, and therefore the 'default' SoA should be extended, by reference to the matrix in §9 of this report. If the organization is subject to other specific regulations then a similar approach could be taken to address any requirements which cannot be readily accommodated by the standard ISMS controls in 27001.

By using the hyper-links between these matrices, and perhaps extended them to their SoA, organizations can easily show how they comply with both 27001 and with HIPAA Security Standards and any other similarly-mapped requirements.

Organizations using Zygma's AIMS, may use the HIPAA Security Standards compliance and ECS pages provided in that tool, which already has these matrices and related linkages installed.

Further information on this tool and other ISMS development and audit support can be requested by contacting the Zygma partnership LLC.

12. Acknowledgements to Peer Reviewers

In common with ISMS practices, it doesn't hurt to get an independent audit of an implementation when you think it is complete, and so some colleagues were asked to review this paper. Their brief was to comment on presentation, readability and to identify any glaring oversights – essentially a sanity check: these individuals do not endorse this paper, nor have they validated the comparative mapping, far too timely a task. Zygma is grateful to the following for their time and wise nudges where they felt this paper could be improved (which, thanks to them, it has been):

Dr. Peter S. ALTERMAN,
Chairman, Federal Public-key Infrastructure Policy Authority (USA)
(www.cio.gov/fpkipa).

Dr. David F.C. BREWER,
Chairman and Managing Director, Gamma Secure Systems Limited (GBR)
(www.gammassl.co.uk)

Mr. Anthony B. NELSON,
President, ESTec Systems Corp. (CAN)
(www.security.estec.com)

Annex A - References

27001	ISO/IEC 27001:2005 "Information Technology – Security techniques – Information security management systems requirements".
17799	ISO/IEC 17799:2005 "Information Technology – Security techniques – Code of practice for information security management".
HIPAA	Health Insurance Portability and Accountability Act 2003 – specifically CFR Title 45 - Part 164 "SECURITY AND PRIVACY", Subpart C, "Security Standards for the Protection of Electronic Protected Health Information".

Digitally signed by Richard G. WILSHER
DN: cn=Richard G. WILSHER, c=US, o=the Zygma partnership LLC, ou=CEO
Reason: Approved for public release
Date: 2006.10.20 04:50:42 Z