HIPAA Implementation Strategies for Small and Rural Providers

By Edward A. Meyer, Attorney at Law
McDonald & Meyer, PLLC
Greensboro, North Carolina

HIPAA Summit West – II
San Francisco, California
The Sheraton Palace Hotel
March 13-15, 2002

Contact information:
(336) 389-9599
www.mcdonaldmeyer.com
emeyer@mcdonaldmeyer.com

HIPAA Summit West – II
San Francisco, California
The Sheraton Palace Hotel
March 13-15, 2002

HIPAA Implementation Strategies for Small and Rural Providers[1]

By Edward A. Meyer, Attorney at Law[2]

I. Introduction

> "The Department [of Health and Human Services] believes that the requirements of the final rule will not be difficult to fulfill, and therefore, it has maintained the two year effective date." 65 FR 82758 (December 28, 2000).

This paper provides guidance on strategies for the implementation of the HIPAA privacy regulation for the small sized "covered entity"[3] under the HIPAA privacy regulations. These small health care providers include entities such as small to medium sized physician practices, rural or county-owned hospitals that are not otherwise affiliates of a larger health system, and other small health care providers with limited budgets, a small administrative staff, and limited resources.

HIPAA guidance for small providers is necessary. Small providers make up 82.6% of all health care establishments in the United States[4] and, thus, are the recipients of a vast portion of the health information that the privacy regulation is intended to protect. See 65 Fed. Reg. 82782 (December 28, 2000). Empirical evidence indicates that many small physician practices have yet to begin their implementation activities. The guidance that is available to these small providers is, for the most part, crafted for the large institutions. The large institution sector of the industry has already dedicated significant resources and

[1] This paper is adapted from a paper delivered by the author to the American Health Lawyers Association meeting in Seattle on December 7, 2001. This paper is being provided for information purposes only is not intended to provide legal advice or to be otherwise relied upon regarding the regulatory requirements of HIPAA.. Persons should consult their legal counsel on questions regarding HIPAA and its requirements. The author specifically disclaims any liability, loss, or risk incurred as a consequence of the use, either directly or indirectly, of any information presented herein.

[2] Mr. Meyer is a founding partner of McDonald & Meyer, PLLC, in Greensboro, North Carolina. Mr. Meyer is licensed to practice law in North Carolina and California.

[3] 45 CFR 160.103 defines "covered entity" to mean "(1) a health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this section.

[4] In the preamble to the final HIPAA privacy regulation, HHS cites reports by the Small Business Administration that there were 562,916 small health care entities in the United States in 1997. 65 Fed. Reg. 82779 (Dec. 28, 2000). These small health care entities make up 82.6 % of all health care establishments in the country, with total revenues of $430 billion, or 30.2 % of total revenues generated by all health care establishments in the United States. Id. at 82779-80.

numerous seminars to the issue of HIPAA implementation for similarly sized entities. The danger, of course, is that policies and procedures that may make sense for large entities may not make sense – and indeed may not even be required – of small entities.[5]

Small providers, especially those in rural areas, have very limited financial, administrative or personnel resources to address HIPAA implementation and compliance. They often have administrative staffs holding only high school diplomas, lack internet access and have outdated computer technology. Thus, they may be reluctant to hire expensive consultants or purchase costly software tools.

Summary of Paper

In order to provide guidance to small providers, this paper reviews the compliance dates under HIPAA and points out that HIPAA safeguard obligations are already in effect. The paper then provides an analysis of the enforcement discretion, scalability and reasonableness provisions in the statute and privacy regulation that may be considered with respect to the obligations of small providers. The paper also provides guidance on educating small providers on strategies for implementing the privacy regulation. The power point presentation that accompanies this paper reviews the work done by a nonprofit consortium of health care providers, payors, clearinghouses, software companies and attorneys in North Carolina to create HIPAA implementation tools and make them available to the health care industry. As part of this review, the powerpoint reviews the HIPAA Earlyview ™ Privacy software tool issued by the North Carolina HealthCare Information and Communications Alliance ("NCHICA").[6]

II. Addressing Implementation Timelines with the Small and Rural Providers

HIPAA Compliance Obligation is Already In Effect

Certain obligations under HIPAA are already in effect. Emphasizing to small providers that they have a current obligation under HIPAA – rather than the far off compliance dates for the regulations -- helps to underscore how important it is for providers of all sizes to take HIPAA compliance seriously.

---

[5] An example of this is the "Tool Kit for Small Group and Safety-Net Providers" prepared for the California HealthCare Foundation. See "HIPAA Administrative Simplification: Tool Kit for Small Group and Safety Net Providers," prepared for the California HealthCare Foundation by the Pacific Health Policy Group (November 2001). While well-intended and including some very excellent recommendations the paper recommends that small groups establish an eleven person HIPAA Steering Committee. That advice is truly impractical for the small physician group or rural hospital who may not even have 11 members of its administrative staff and whose attorney combines his or her time with a myriad of non health care law related matters.

[6] This paper describes NCHICA's HIPAA Earlyview™ Privacy software. McDonald & Meyer, PLLC is a member of NCHICA. Neither Mr. Meyer nor McDonald & Meyer, PLLC have any ownership rights in that software.

Under the HIPAA statute, covered entities have a current statutory obligation to maintain safeguards "to ensure" the integrity and confidentiality of health information, to protect the security and integrity of that information and "to ensure" the compliance by their officers and employees. See 42 U.S.C. Sec. 1320d-2(d). In pertinent part, Section 1173 of the Social Security Act, enacted as part of the 1996 HIPAA legislation, provides that "Each person described in section 1320d-1(a) of this title who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safeguards" (a) "to ensure the integrity and confidentiality of the information;" (b) "to protect against any reasonably anticipated . . . threats or hazards to the security or integrity of the information" and "unauthorized uses or disclosures of the information"; and (c) otherwise to ensure compliance with HIPAA by their officers and employees. 42 U.S.C. Sec. 1320d-2(d). Section 1320d-1(a) is the statutory definition for "covered entity" under the HIPAA regulations. See 42 U.S.C. Sec. 1320d-1(a); cf. 45 CFR 160.103. Unlike the privacy regulations, which require compliance beginning April 14, 2003,[7] the general statutory obligation became effective upon the 1996 enactment of the Health Insurance Portability and Accountability Act.

Thus, HIPAA imposes current obligations on covered entities implement safeguards to protect the confidentiality and security of health information.

III. Reasonableness, Scalability and Enforcement Restrictions: Considerations for Legal Counsel Analyzing the Regulations

Overview

When focusing upon how small entities can implement the privacy regulations, it is important to recognize that the regulations were drafted with the understanding that regulations extend to small entities.

The HIPAA privacy regulations reflect a flexibility that is intended to facilitate small entity compliance with the regulations. The principle that the regulations should be flexible is reflected in the enforcement provisions of the HIPAA statute. In addition, many requirements of the final HIPAA privacy regulations are "scalable." [8] Others include an objective "reasonable efforts" qualifier.[9] The flexibility found within the specific terms of the standards and specifications in the Privacy regulation should be considered by counsel when designing or identifying policies, procedures and forms, as well as when determining the compliance obligations of their small provider clients. It

[7] By April 14, 2003, covered entities must meet the HIPAA privacy standards in order to use, maintain or disclose protected health information in treatment, business operations or other activities (small health plans have until April 14, 2004).

[8] See the discussion under the header, "scalability," below.

[9] See 45 CFR 164.502(b)(1); and 45 CFR 164.514(d) [re minimum necessary rules]; and 45 CFR 164.504 (e)(1)(ii) [regarding a covered entity's obligation to take "reasonable steps" to mitigate the harm caused by a breach of a business associate of privacy standards].

should be considered when counsel evaluates whether a particular implementation specification requires a complex policy or procedure, or whether a simpler approach may be permitted under the regulations.

Enforcement Discretion

The enforcement provisions of the Administrative Simplification provisions of HIPAA specifically provide the Secretary with discretion when determining civil monetary penalties and even authorize the Secretary to offer assistance to providers in their compliance efforts.

The HIPAA Statute prohibits its civil monetary penalties from being imposed in the following instances:

(a) "if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision." 42 U.S.C. 1320d-5(b)(2); and

(b) if "(i) the failure to comply was due to reasonable cause and not to willful neglect; and (ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred." 42 U.S.C. 1320d-5(b)(3)(A).

The foregoing enforcement provisions may be helpful for small providers with limited budgets that have difficulty complying with the complex privacy regulations.

The HIPAA statute's Civil Monetary Penalty provision also provides the Secretary with significant discretion to assist covered entities that have difficulty complying with HIPAA safeguard obligations. This includes:

The Secretary has the discretion to extend the 30 day correction period of 42 U.S.C. 1320d-5(b)(3)(A) "as determined appropriate by the Secretary based on the nature and extent of the failure to comply." 42 U.S.C. 1320d-5(b)(3)(B)(i);

If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the correction period. Such assistance shall be provided in any manner determined appropriate by the Secretary. 42 U.S.C. 1320d-5(b)(3)(B) (ii); and

In the case of a failure to comply with HIPAA that is due to reasonable cause and not to willful neglect, the Secretary may waive payment of the HIPAA civil monetary penalty would be excessive relative to the compliance failure involved. 42 U.S.C. 1320d-5(b)(4)

These provisions of the HIPAA statute, in effect, authorize HHS enforcement officials to be lenient with providers that have difficulty meeting the regulatory obligations. These statutes permit HHS to provide the necessary implementation assistance to a provider with limited resources or unsophisticated support staff as the provider attempts to bring itself into HIPAA compliance.

The providers, of course, must attempt compliance in order to avail themselves to this leniency. In addition, local governments in underserved areas may want to consider citing these provisions as they appeal to HHS regional offices for assistance to their local health care provider community.

Significantly, the Secretary has expressed a willingness to use discretion in enforcement:

> "As to enforcement, a covered entity will not necessarily suffer a penalty solely because an act or omission violates the rule. As we discuss elsewhere, the Department will exercise discretion to consider not only the harm done, but the willingness of the covered entity to achieve voluntary compliance." 65 Fed. Reg. 82603 (December 28, 2000).

Scalability

When it issued the final privacy regulation, the Department of Health and Human Services made a conscious effort to keep the rules flexible in order to facilitate implementation by covered entities of various sizes. [10] The Department purposefully drafted the regulations so that many implementation specifications were flexible and scalable to reflect the array of covered entities regulated. [11] This principle of "scalability" is found in numerous provisions of the regulation.[12] It was also restated in

[10] "[W]e recognize that the cost of implementing privacy provisions could be a larger burden to small entities as a proportion of total revenue [than for large business]. Due to these concerns, we have relied on the principle of scalability throughout the rule, and have based our cost estimates on the expectation that small entities will develop less expensive and less complex privacy measures that comply with the rule than large entities." 82785

[11] "The vast difference among regulated entities also informed our approach in significant ways. This regulation applies to solo practitioners, and multi-national health plans. It applies to pharmacies and information clearinghouses. These entities differ not only in the nature and scope of their businesses, but also in the degree of sophistication of their information systems and information needs. We therefore designed the core requirements of this regulation to be flexible and ``scalable." This is reflected throughout the rule, particularly in the implementation specifications for making the minimum necessary uses and disclosures, and in the administrative policies and procedures requirements." 65 Fed Reg. 82471 (December 28, 2000).

[12] See e.g. 45 CFR 164.502(b) and 164.512(d) [regarding "minimum necessary" disclosures]; 164.528(b) [regarding the lack of specificity required in the accounting record keeping]; and 164.530(a) [designation of a privacy official]; 164.530(d)(1) [documentation of complaints].

the July, 2001, HHS guidance on the privacy regulation.[13] Scalability permits smaller providers to implement the regulation with consideration of their size and resources.

The basis for use of this flexible "scalability" approach to the regulation may lie in the fact that health information is held by both large and small providers. The size and sophistication of a provider will dictate its actual ability to comply with complex regulations.[14]

The Department's concern that the regulations must be "scalable" provides ample persuasive authority to interpret scalable provisions to the benefit of small providers. Examples of the Department's concern about the need for scalability is reflected in the following comments in the preamble to the Privacy regulation:

> "We do not prescribe the particular measures that covered entities must take to meet this standard, because the nature of the required policies and procedures will vary with the size of the covered entity and the type of activities that the covered entity undertakes. (That is, as with other provisions of this rule, this requirement is ``scalable.")" 65 Fed. Reg. 82562 (December 28, 2000).
>
> "In Sec. 164.530(i) [regarding the standard for policies and procedures] we require that the policies and procedures be reasonably designed to comply with the standards, implementation specifications, and other requirements of the relevant part of the regulation, taking into account the size of the covered entity and the nature of the activities undertaken by the covered entity that relate to protected health information." 65 Fed. Reg. 82563 (December 28, 2000).

In addition, within the context of the discussions of "scalability," the Department appears to have attempted to draft particular standards to fit within current business practices of small providers so as to make implementation simpler. These comments in the preamble also provide persuasive authority regarding how current practices should be viewed in light of the regulations.

---

[13] See U.S. Department of Health and Human Services, Office of Civil Rights, "Standards for Privacy of Individually Identifiable Health Information," (July 6, 2001) (accessible at the following link: http://www.hhs.gov/ocr/hipaa/finalmaster.html) ("[T]he Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the rules provides a more efficient and appropriate means of safeguarding protected health information than would any single standard.")

[14] See 65 Fed. Reg. 82749 (December 28, 2000). ("We do not include more specific guidance on the content of the required policies and procedures because of the vast difference in the size of covered entities and types of covered entities' businesses. We believe that covered entities should have the flexibility to design the policies and procedures best suited to their business and information practices. We do not exempt smaller entities, because the privacy of their patients is no less important that the privacy of individuals who seek care from large providers. Rather, to address this concern we ensure that the requirements of the rule are flexible so that smaller covered entities need not follow detailed rules that might be appropriate for larger entities with complex information systems.")

> "For small health care providers that are covered health care providers, we expect that they will not be required to change their business practices dramatically because we based many of the standards, implementation specifications, and requirements on current practice and we have taken a flexible approach to allow scalability based on a covered entity's activities and size." 65 Fed. Reg. 82785 (December 28, 2000).
>
> "Wherever possible, the final rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the standards, implementation specifications, and requirements of the rule." 65 Fed. Reg. 82782 (December 28, 2000).

These passages from the preamble to the Privacy Regulation provide significant guidance regarding the flexible approach HHS plans to take on implementation. It indicates that providers should consider modifications to their current practices – rather than wholesale change – as a way to bring themselves into compliance with the privacy regulations.

Reasonableness

In addition to the flexibility afforded covered entities under scalable provisions of the regulations, some provisions of the privacy regulation incorporate a "reasonable efforts" qualifier to their requirements. Such a qualifier may be helpful to small providers, since efforts that may be reasonable to a large health system to perform may be unreasonable to require of a small health care provider.

Many small providers, as well as large institutions, may mistakenly believe that they merely need to use "reasonable efforts" to meet the privacy regulations.

A review of the regulation, however, indicates that there is no general rule within the Privacy Rule that covered entities need only make reasonable efforts to meet the HIPAA Privacy Rule standards or implementation specifications.

Instead, the "reasonable efforts" type qualification is provision specific.

For example, the "Minimum Necessary" disclosure Standards generally requires that "When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make *reasonable efforts* to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." 45 CFR 164.502(b)(1) (emphasis added); see also 45 CFR 164.514(d).

The regulation permits covered entity to restrict disclosures to the personal representatives of unemancipated minors when the covered entity has a "*reasonable belief*" that treating the person as a personal representative poses a danger to the minor.

See 45 CFR 164.502 (g)(5) (but note that the President and the Secretary have indicated that these provisions may be modified with respect to parental rights).[15]

When a business associate agreement HIPAA provisions are breached, the covered entity must take "*reasonable steps* to cure the breach or end the violation . . ." 45 CFR 164.504 (e)(1)(ii) (emphasis added).

A covered entity must make "reasonable efforts to ensure" that individuals that opt out of receiving future marketing or fundraising communications are not sent such communications. 45 CFR 164.514(e)(3)(iii) and (f)(2)(ii).[16]

"Reasonable efforts" are also required with respect to the obligation of the covered entity to inform certain individuals that a patient request for amendment to his or her protected health information ("PHI") has been made. 45 CFR 164.526(c).

A "reasonableness" standard appears with respect to the overall requirement regarding the safeguards that a covered entity must put into place for protected health information:

A covered entity must "reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart." 45 CFR 164.530(c)(2).

Additional "flexibility" factor

In addition to scalability and reasonableness standards, counsel should also consider the opening quote of the paper: Since the Secretary of Health and Human Services believes that "the requirements of the final rule will not be difficult to fulfill," counsel might consider using that guidance as persuasive authority when analyzing whether a vague provision of the regulation requires the implementation of a complex or burdensome policy or whether a more simpler approach may suffice.

IV. Implementation Guidance: A Suggested Approach for Small and Rural Providers.

As discussed above, for the small provider with limited resources, it is imperative for legal counsel or the small practice HIPAA consultant to convey the importance of compliance. The privacy regulations are far reaching and failure to comply with the regulations exposes the covered entity to civil and criminal penalties under the HIPAA

[15] See the July 8, 2001 HHS Guidance on the HIPAA Privacy Rule, available at http://www.hhs.gov/ocr/hipaa/index.html#Initial Guidance; (a direct link to the discussion on the relationship of parents and minors under the rule can be accessed at http://www.hhs.gov/ocr/hipaa/minors.html).

[16] HHS has issued guidance and frequently asked questions regarding the privacy regulation's restrictions on the use of protected health information in marketing at http://www.hhs.gov/ocr/hipaa/marketing.html.

statute, as well as raising the specter of private causes of action under various state tort theories for breaches of an individual's right to keep their health information private.

A good implementation strategy uses the following steps: (1) summarize the rule in the briefest way possible; (2) provide a general education on the HIPAA privacy regulation; (3) break the rule down to its basic components and highlight where the regulation is both flexible and includes requirements that the provider may already be performing; (4) assist the provider in performing a gap analysis, including assessment checklists and use of an available software tool; and (5) identify where form policies, procedures and contracts may be used by the practice to meet HIPAA privacy regulations requirement and assist the health care provider in using them to implement the regulation.

This, of course, is only a suggested approach. Other approaches have been suggested. For example, the WEDi-SNIP White Paper on Small Practice Implementation suggests a preliminary HIPAA awareness effort focused upon the basic requirements of the regulations delivered in a "simple, straightforward, and . . . non-technical" manner that also includes the use of a self-assessment checklist. Form documents would then be made available to small practices by "trusted sources" (such a regional SNIPs, local government agencies, provider associations, and payors) so that the Practice could adopt them, after some modifications, to fit their needs.

WEDi-SNIP's emphasis on the need to avoid technical HIPAA jargon when discussing HIPAA with small providers is commendable, but should also be guidance for educating the employees of large institutions. Their suggestion that a self-assessment be done as an initial step is also commendable, but users of this approach should be careful that this self-assessment not cause the provider to focus too quickly on the trees instead of understanding the structure of the forest.

Step One: Be Brief: Convey that the HIPAA Regulations Are About "Standards"

The first step of such process is to summarize these complex privacy rules in as succinct a statement as possible. The chief executives of small providers, such as the physician owner of a small practice, are often very busy and focused on multiple priorities for their organization. A brief summary of the purpose and intent of the privacy regulations is extremely helpful in getting the executive to focus on why implementation is important and what implementation efforts will entail. Simplicity is at the core of the efforts to implement complex policies and procedures.

Consider the following summary of the privacy regulations:

> The HIPAA final privacy regulations establish national standards[17] to protect the privacy of individually identifiable health information held, used or disclosed by

[17] The authority and directives given to HHS by statute to issue what became the voluminous final HIPAA privacy regulation can be found in a few short paragraphs of the "Administrative Simplification" title of the Health Insurance Portability and Accountability Act of 1996. In pertinent part, the Act provides that "If legislation governing standards with respect to the privacy of individually identifiable health information

health care providers. Failure to meet these standards permit the government to impose civil and criminal penalties and opens the door for private lawsuits by patients who allege that their health information was not protected adequately by the covered entity.

An alternative summary can be found in the WEDi-SNIP Small Practice Implementation White Paper:

> "The administrative simplification provisions of HIPAA have two parts:
>
> - Development and implementation of standardized electronic transactions; and
>
> - Implementation of privacy and security procedures to ensure the confidentiality of and prevent misuse of patient information."[18]

Step Two: Educate

After the key decision makers of the covered entity are able to focus upon the underlying purpose of the privacy regulation, the second step in implementation strategy is to educate those assigned the task within the covered entity to implement the general requirements of the regulation. This should include at least one owner of the entity (or senior manager) and a key administrative person, such as the office manager. The goal of such education is not to make the these individuals "HIPAA experts."

This education can be done at relatively little expense. There are both government sources and private sector sources where initial HIPAA education is available at little or no cost to the provider.

The Office of Civil Rights at the U.S. Department of Health and Human Services has indicated that it will make videos available summarizing the rule. In addition, there are a number of briefing papers and fact sheets available on the Department of Health and Human Services' web site (www.dhhs.gov) that explain the regulations in very brief terms. The web pages for the Office of Civil Rights at the U.S. Department of Health and Human Services (http://www.hhs.gov/ocr/hipaa/) include excellent summaries. This web

---

transmitted in connection with [the standards to enable health information to be exchanged electronically], is not enacted [by Congress by a date certain], the Secretary of Health and Human Services shall promulgate final regulations containing such standards . . ." Public Law 104-191, Section 264(c). The authorizing statute directs HHS that "Such regulations shall at least address" the following subjects: "(1) the rights that an individual who is a subject of individually identifiable health information should have; (2) the procedures that should be established for the exercise of such rights; and (3) the uses and disclosures of such information that should be authorized or required." Id. at Section 264 (b) and (c). Understanding that these three subjects are at the core of standards issued as the final privacy regulations is essential in simplifying those regulations for the small provider.

[18] WEDiSNIP, "Small Practice HIPAA Implementation," Version 1.0 – 12/12/2001 Discussion Draft, at page 2. This paper can be found at Available at http://snip.wedi.org/public/articles/smallpractice.pdf.

site includes a copy of the 36 page guidance issued by HHS on July 6, 2001. That initial guidance provides practical responses to many common questions asked about implementing the privacy regulation.

On the private sector side, the powerpoint presentations delivered at the annual HIPAA Summit and other national conferences are also available on the conferences' web sites. See (www.hipaasummit.com).

Another excellent initial education tool is the "Small Practice Implementation" White Paper being published by the Workgroup for Electronic Data Interchange Strategic National Implementation Process (WEDi-SNIP).[19] The White Paper includes very brief and common-language descriptions of the HIPAA Transactions and Code Sets standards, the proposed Security Rules and the final Privacy Rules. The paper also includes a "privacy and security audit for small practices" checklist that runs through numerous scenarios on how the HIPAA regulations impact every day practices of a small physician group.[20]

Step Three: Break Up the Privacy Rule to its Essential Tasks and Identify Scalability[21]

The third step in the implementation strategy is to convey to the small provider that the privacy regulation can be broken down to simpler provisions, many of which require documents to be implemented. Under each of these provisions are the more complex standards and implementation specifications. Counsel should identify the scalability permitted within each, and also identify where good sample forms, policies, procedures and contracts applicable to a particular component may be available. Such identification is imperative to reduce the costs of implementation and to avoid the need to "reinvent the wheel" with regard to a particular implementation specification, provided that the form fits within the activities of the particular entity.

By breaking down the regulation to its core required implementation actions, implementation may be more manageable – and the regulation more understandable – for small providers.

The regulation generally can be broken down into 12 distinct tasks as follows:

1. Appoint a Privacy Officer and assign duties. The regulation is brief: "A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity." 45 CFR 164.530(a)(1). No other specific duties are described in the regulation.

---

[19] WEDiSNIP, "Small Practice HIPAA Implementation," Version 1.0 – 12/12/2001 Discussion Draft. This paper can be found at Available at http://snip.wedi.org/public/articles/smallpractice.pdf.

[20] Id. at Appendix I.

[21] The author acknowledges the work performed by NCHICA's HIPAA Implementation Task Force in developing the 12 key components of the privacy regulation. The work to summarize each element and to describe the scalable aspects below each element are that of the author of this paper.

The following scalable aspects of this requirement are notable:

(a) Duties are general in nature. See 45 CFR 164.530(a).

(b) Designating the office manager as privacy official and adding privacy-related duties are permissible. 65 Fed. Reg. 82783 (December 28, 2000).

(c) "We expect implementation to vary widely depending on the size and nature of the covered entity, with small offices assigning this as an additional duty to an existing staff person, and large organizations creating a full-time privacy official." 65 Fed. Reg. 82561 (December 28, 2000).

2. Adopt a notice of privacy practices. The requirements of this notice are specified in the regulations at 45 CFR 164.520. While they appear complex, they lend themselves to the use of form notices that meet the regulatory requirements.

The following scalable aspects of this requirement are notable:

(a) The notice can be based on a form notice that is modified for use by the particular covered entity.

(b) Consider whether model forms have been developed by professional or trade association of which the small entity is a member.

(c) In order to meet the requirement that each patient receives copy of the notice of privacy practices, consider the following guidance from HHS: "We expect that providers will simply place a note or marker at the beginning of a file (electronic or paper) when a patient is given the notice. This is neither time-consuming nor expensive, and will not require constant searches of records." 65 Fed. Reg. 82757 (December 28, 2000).

3. Adopt a HIPAA Consent form for Treatment, Payment and Health Care Operations. The privacy regulations permit a covered entity to use or disclose protected health information to carry out treatment, payment, or health care operations if the use or disclosure is pursuant to and in compliance with a consent that complies with 45 CFR 164.506. See 45 CFR 165.402(a)(1)(ii). The required provisions of the consent are described at 45 CFR 164.506 and can be easily incorporated into a form consent, many of which forms have already been developed.

Summary guidance and answers to frequently asked questions regarding the consent requirements have been issued by the HHS Office of Civil Rights.[22]

[22] See U.S. Department of Health and Human Services, Office of Civil Rights, "Standards for Privacy of Individually Identifiable Health Information" (July 6, 2001) (a direct link to the text on consents is available at http://www.hhs.gov/ocr/hipaa/consent.html)

The following scalable aspects of this requirement are notable:

(a) Consider using a form consent, tailored for particular covered entity.

(b) Consider whether model forms developed by professional or trade association may be used.

4. Adopt a HIPAA Authorization form. The privacy regulation permits a covered entity to use or disclose protected health information pursuant to and in compliance with a valid authorization under 45 CFR 154.508. See 45 CFR 164.502(a)(1)(iv). Since consents are required for use or disclosures involving treatment, payment and health care operations, authorization are generally required in most other instances where protected health information is used or disclosed. Like the consent requirements, the authorization provisions are detailed with respect to the information that must appear in the authorization. Forms, however, may be used, provided that they meet the requirements of the regulation.

   The following scalable aspects of this requirement are notable:

   (a) The authorization can be based on form authorization (with space to add required specificity), updated for a particular practice.

   (b) Consider using a form developed by a professional or trade association for a similar organization.

5. Obtain patient Consents and Authorizations under adopted forms. Since these will need to be in place by the April 14, 2003 compliance date in order for practices to generally use or disclose protected health information, the practice will need to put a mechanism in place so that new or returning patients complete the required paperwork or that entities in which a physician obtains, uses or discloses protected health information will have the required consents or authorizations in place.

6. Identify all "Business Associates," adopt a form contract and enter into a Business Associate Agreements with all "Business Associates." A covered entity is permitted under the privacy regulation to disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. 45 CFR 165.502(e)(1). The standards and implementation specifications for business associate arrangements are described at 45 CFR 165.504(e). While these required elements of a business associate contract are complex, they lend themselves to the use of form contractual addenda.

The requirement that contracts with business associates must be modified to comply with the privacy regulations will require early identification of the contracts that fall within the definition of "business associate arrangements" under the regulation.

Prior to the compliance date, the covered entity must make requests for amendment to these contracts as they are renewed or renegotiated, and accomplish the required amendments. Since business associates are likely to contract with other covered entities, professional or trade associations should be utilized to establish a generally accepted form addendum, thus reducing the cost of compliance.

Summary guidance and answers to frequently asked questions regarding the business associate provisions in the privacy rule have been issued by the Office of Civil Rights[23]

The following scalable aspects of this requirement are notable:

(a) Standard contract forms can be used. 82 Fed. Reg.82785.

(b) There is no specific regulatory requirement on covered entity that they monitor actively their business associate's compliance. See . 65 Fed Reg. 82785 (December 28, 2000).

(c) Covered entity's obligation to mitigate harm is qualified "to the extent practicable." 45 CFR 164.530

7. Adopt policies & procedures to handle patient requests regarding their protected health information. Covered entities are required to permit an individual to make certain requests regarding their own protected health information, such as placing restrictions on the use or disclosure of the information (45 CFR 164.522), requesting access to inspect and obtain a copy of the information (45 CFR 164.524), to request an amendment be made to their information (45 CFR 164.526), and to receive an accounting of certain disclosures of their protected health information (45 CFR 164.528). Each of the above-cited regulatory references describes the standards and implementation specifications required to accommodate each such request. Form policies and procedures can be used to implement the complex requirements of the regulations.

The following scalable aspects of this requirement are notable:

(a) No requirement that Covered Entities actually rewrite or correct records to reflect patient's requested amendment.

[23] See U.S. Department of Health and Human Services, Office of Civil Rights, "Standards for Privacy of Individually Identifiable Health Information" (July 6, 2001) (a direct link to the text on consents is available at http://www.hhs.gov/ocr/hipaa/busassoc.html)

(b) A covered entity may "append" the record (i.e., add a note in the record on any comments from the patient).

(c) The policies and procedures to accommodate the request may be similar to an organizations current practices such that the organization should consider modifying current practices to meet the regulatory requirements.

(d) Consider adopting model policies from professional or trade associations. ("[T]he Department expects many professional and trade associates to provide their members with . . . model policies, statements and basic training materials.") 65 Fed. Reg. 83756 (December 28, 2000).

8. Adopt policy regarding "Minimum Necessary" disclosures. When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity is required under the regulation to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This minimum necessary requirement does not apply to disclosures to or requests by a health care provider for treatment; uses or disclosures made to the individual (with certain exceptions); pursuant to an authorization (except for certain authorizations); certain disclosures to the Secretary; uses or disclosures that are required by law; and uses or disclosures that are required for compliance with applicable requirements of the privacy regulation. See 45 CFR 164.502(b). The standard and implementation specifications for this "minimum necessary" rule are described further at 164.514(d).

Summary guidance and answers to frequently asked questions regarding this "minimum necessary" requirement have been issued by the HHS Office of Civil Rights. [24]

The following scalable aspects of this requirement are notable:

(a) HHS believes that the rule is similar to the current practice of many providers. 65 Fed. Reg. 82783 (December 28, 2000).

(b) The three basic components of the minimum necessary rule are (1) the rule does not pertain to uses and disclosures including treatment-related exchange of information among health care providers; (2) for disclosures that are made on a routine basis, such as insurance claims, a covered entity

[24] See U.S. Department of Health and Human Services, Office of Civil Rights, "Standards for Privacy of Individually Identifiable Health Information" (July 6, 2001) (a direct link to the text addressing the "minimum necessary" requirement is available at http://www.hhs.gov/ocr/hipaa/minnec.html) ("HHS emphasizes that "[t]his is not a strict standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers today to limit the unnecessary sharing of medical information.").

is required to have policies and procedures governing such exchanges. No case-by-case determination is needed for such disclosures; and (3) providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed. See 45 CFR 164.514(d)(4); and 65 Fed. Reg. 82782.

9. Train all employees on HIPAA privacy standards, policies & procedures. A covered entity is required to train all members of its workforce on the policies and procedures with respect to protected health information, "as necessary and appropriate" for the members of the workforce to carry out their function within the covered entity. 45 CFR 164.530(b)(1). The implementation specifications describe when employees must receive their training and the documentation required that such training occurred. See 45 CFR 164.530(b). The regulations, however, do not otherwise specify what must be contained within the training.

   The following scalable aspects of this requirement are notable:

   (a) "[T]he final rule leaves to the employer the decisions regarding the nature and method of training to achieve this requirement. The Department expects a wide variety of options to be made available by associates, professional groups, and vendors. Methods might include classroom instruction, videos, booklets, or brochures tailored to particular levels of need of workers and employers." 65 Fed. Reg. 82783 (December 28, 2000).

10. Amend employee manual regarding the HIPAA privacy rules. Since the HIPAA privacy regulations require various policies and procedures to be in place in order to protect the privacy of individually identifiable health information, employee manuals will need to be updated to reflect these policies and procedures.

    The following scalable aspects of this requirement are notable:

    (a) "Small providers will be able to develop more limited policies and procedures under the rule, than will large providers and health plans, based on the volume of protected health information." 65 Fed. Reg. 82783 (December 28, 2000).

11. Implement HIPAA security safeguards. As of February 14, 2001, the HIPAA security regulations have only been issued in proposed form. The final privacy regulation, however, requires that a covered entity must have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 CFR 164.530(c)(1); cf. 42 U.S.C. 1320d-2(d) (requiring that covered entities maintain "reasonable and appropriate administrative, technical, and physical safeguards . . . to ensure the integrity and confidentiality of the information").

The implementation specifications require the covered entity to "reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart." 45 CFR 164.530(c)(2). No specific safeguards are described in the final regulation.

Summary guidance and answers to frequently asked questions regarding the obligations to safeguard against disclosures have been issued by the Office of Civil Rights[25]

12. Adopt HIPAA privacy compliance record-keeping policies, including means to meet disclosure accounting requirement. A covered entity is required to keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary of Health and Human Service may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements, standards and implementation specifications of the privacy regulations. 45 CFR 160.310. Disclosure accounting requirements are described at 45 CFR 164.528.

The privacy regulations place extensive documentation requirements on covered entities. See generally 45 CFR 164.530 (j). The covered entity must retain the signed consents (45 CFR 164.506(b)(6)); the signed authorizations 45 CFR 164.508 (b)(6)); and copies of the notices of privacy practices (45 CFR 164.420(e)). If it obtains an individual's preference with respect to resolving a conflict between a consent and an authorization, the covered entity must document the preference. See 45 CFR 164.506 (e) (2) (ii). When a consent is not obtained under the emergency treatment exception, or when the covered entity treats a patient because it is required by law to do so, or when substantial barriers restrict the ability to obtain consent, then the covered entity must document its attempts to obtain the consent. See 45 CFR 164.506 (a)(3)(ii). A covered entity that agrees to a patient request to restrict disclosure of PHI must document the restriction in accordance with 45 CFR 164.530(j). See 45 CFR 164.522(a)(3). Documentation may also be required when a covered entity terminates at the patient's request a restriction placed by the patient on disclosure of PHI. See 45 CFR 164.522 (a) (2) (ii). In addition, a covered entity must document and retain the documentation as required by Sec. 164.530(j) of the designated record sets that are subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access by individuals. See 45 CFR 164.524(e). It must also document the titles of persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by Sec. 164.530(j). See 45 CFR 164.526 (f). Training must be documented. See 45 CFR 164.530 (b) (2) (ii). Complaints and their disposition must be documented. See 45 CFR 164.530 (d)(2). Sanctions

[25] See U.S. Department of Health and Human Services, Office of Civil Rights, "Standards for Privacy of Individually Identifiable Health Information" (July 6, 2001) (a direct link to the text on consents is available at http://www.hhs.gov/ocr/hipaa/oral.html).

must be documented. See 45 CFR 164.530 (e) (2). It must document changes to its policies and procedures. See 45 CFR 164.530 (i) (2) (iii); (i) (4); and (i) (5). Also, whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. See 45 CFR 164.530 (i) (3).

The following scalable aspects of this requirement are notable:

(a) The record keeping of disclosures can be done by notation in the medical record. 65 Fed. Reg. 82784 (December 28, 2000).

(b) Consider ways these documentation requirements can be placed in a checklist for the organization.

(c) Consider the most logical places in the organization where these documents may be retained.

Step Four: Gap Analysis

As discussed above, the key decision makers of the entity who are charged with implementing the privacy regulation should be educated about the general requirements of the regulations. The rule needs to be simplified and broken down to its basic components in order to facilitate both understanding of the rule and the identification by the organization where it may already be performing activities similar to requirements under the privacy regulation. Compartmentalizing the regulation may provide a manageable framework for the organization to understand the regulation as it applies to its day-to-day operations. A gap analysis can works as a further education tool by applying the rules to a specific set of situations and asking whether the provider meets the requirement in the situation.

The next step in the implementation strategy is for the organization to identify where it already has policies and procedures in place that need modifying (or which may already comply) and where additional HIPAA compliant practices need to be implemented. This "gap" analysis can be used to generate a report that identifies the actions that the practice needs to undertake to implement the regulation.

This assessment can be done either comprehensively or in two steps. A comprehensive approach would be to use one of the available software tools and work through an assessment of how the practices and procedures currently existing with the practice stand up to the final privacy regulation. The two step approach is to do an initial assessment with a simple checklist and then move on to a more comprehensive gap analysis.

The advantage of the two step approach is that the initial assessment is relatively straight forward to perform and begins the process of understanding the practical impact of the privacy regulations. For small physician groups with limited resources, this simple checklist approach may make sense. A sample checklist can be found in the WEDi-

SNIPA White Paper on "Small Practice Implementation." The down-side of the use of initial checklists is that the checklists describe HIPAA standards in the briefest of terms and tend to focus only on the obvious confidentiality issues. A "yes" answer to a checklist question whether a particular policy is in place may mislead the small provider into believing it has complied with the particular HIPAA standard. A good example is the issue of consents: a HIPAA provider may believe that language in its consent to treatment form satisfies the general HIPAA privacy consent requirement. That requirement, however, specifically requires HIPAA privacy consents to be signed separately from other consent forms. Such a distinction, however, may not be discerned from the checklist.

With regard to the comprehensive gap analysis approach, a number of software tools are available to assist providers. The costs of these tools vary greatly and many may be oriented more toward the large entity health care provider rather than smaller entities. Many of these tools include sample forms. These tools include HIPAABasics (www.hipaabasics.com), considered by at least one consultant who has reviewed a number of HIPAA gap analysis software tools to be one of the "'Cadillacs" of compliance tools.[26] Other tools include the HIPAA Monitor (http://www.hipaamonitor.com); HIPAA Earlyview™ Privacy (discussed in detail below), the HIPAA Calculator http://www.privacysecuritynetwork.com; and HealthFlash, (http://www.healthflash.net).

The advantage to a number of these tools is that they provide a user friendly software program that permits users to be walked through the requirements of the privacy regulations in an orderly fashion so as to identify where in the organization remedial action must be taken to bring the practice into HIPAA compliance. Many permit the generation of a report that can be used as a guide for future action items to implement the regulation.

Step Five: Identify Forms and Implement in accordance with gap analysis report.

As part of any remediation plan, the organization will need to adopt policies and procedures, forms, notices and contracts that comply with the regulations. In many instances, generally accepted forms created through professional or trade associations can be used. While there may be a wide array of forms floating around on the internet, it is important to consider whether or not the forms actually meet the standards established under the HIPAA privacy regulations. In addition, especially with regard to form business associate agreements, it is also important to consider whether the available forms are written with a particular type of covered entity in mind. An excellent source of forms that have been worked on through the efforts of a broad array of covered entities, consultants and attorneys are the forms available through The North Carolina Healthcare Information and Communications Alliance (NCHICA). The NCHICA web site is www.nchica.org. For counsel who is advising clients on the development of their own

[26] See Sommerville, "Unscrambling HIPAA – New software helps physicians, business digest complex rules," The Business Journal Serving the Greater Triad Area (week of Nov. 12, 2001) (http://bizjournals.bcentral.com/triad/stories/2001/11/12/focus1.html)

unique forms, HIPAA compliance checklists are also available through NCHICA for a wide variety of documents required under the privacy regulation.

WEDi-SNIP's web site also includes model forms, as do the web sites for the American Medical Association and American Hospital Association.

V. HIPAA Earlyview™ Privacy – A Gap Analysis Tool Focused on the Small Provider[27]

The Powerpoint presentation that accompanies this paper includes a review of this sample gap analysis software tool for use in education on and implementation of the privacy regulations. HIPAA Earlyview™ Privacy is a self-assessment software tool for physician practices and others covered by the HIPAA privacy regulation. This software developed by the North Carolina Healthcare Information and Communications Alliance ("NCHICA") in conjunction with the State of Maryland Health Care Commission ("SMHCC") and builds upon the SMHCC's work to summarize and organize the implementation requirements of the privacy regulation. NCHICA is a non profit, volunteer driven consortium that is composed of various sectors of the health care and consulting field, both inside and outside of North Carolina.

The tool includes the following:

33 Requirements from the Privacy Rule

43 Questions keyed to Requirements

Incorporates industry "best practices"

Includes recommended "action items" to fulfill each Requirement

Links to online sample documents, document portfolio management facility

Includes cross references to regulations, definitions, and related requirements within HIPAA

User Guide

The tool permits reports to be run assessing implementation status.

This tool is an example of software available from various sources.

[27] Discussion in this paper of either the HIPAA Earlyview ™ Privacy tool or documents available through NCHICA does not constitute any endorsement or recommendation of these tools or documents by the author or by McDonald & Meyer, PLLC. The author is describing these for the purpose of describing an example of work done by collaborative effort to address HIPAA implementation. The author discloses that he participated in the development of the HIPAA Earlyview ™ Privacy tool but has no ownership interest in the tool or in NCHICA. McDonald & Meyer, PLLC is a member of NCHICA.