HIPAA Best Practices?

Roy Rada, M.D., Ph.D.
University of Maryland, Baltimore County
Baltimore, MD 21250
rada@umbc.edu

Abstract

The term 'best practices' is often prematurely applied to HIPAA compliance practices. Identifying common practices for HIPAA is a precursor to determining best practices. A taxonomy is proposed for HIPAA practices and tools. An ad hoc inventory of existing practices reveals that small entities should have distinctly different practices from large entities. Patterns of tool usage suggest that simple tools are most popular. Paths to further sharing may depend most on the support of the government.

1 Introduction

Achieving HIPAA compliance is a massive national task that is largely being approached in a piecemeal fashion. To what extent can entities share experiences and help one another? Would this constitute adopting best practices? What is the difference between common practices and best practices?

Two common ways of defining best practice are (Keehley et al, 1997):

- Some consider a best practice anything better than their current practice. When practitioners learn about new ideas or practices, they frequently refer to them as best practices. The term is popular and suggests a best way has been found. In this same vein, some consider a best practice to be any emerging industry trend that seems to make sense. This interpretation of best practice fails to appreciate the importance relationships among a context, performance results, and any practice being considered.

- Another common meaning of 'best practices' is something declared by others to be a 'best practice'. The media run articles on current practices to showcase the successes of organizations. A best practice is seen as some action that helped an organization overcome an obstacle. For instance, the Department of Veterans

Affairs hired a consulting firm to compile a list of best practices. The firm interviewed industry experts on what they saw as best, but the criterion was solely the judgment of experienced people. A best practice should involve measurable attributes.

The research on best practices has been imprecise. The term 'best practices' should not mean simply sharing practices and making comparisons. Best practices should be

- quantifiably successful over a prolonged period and
- repeatable with modification in similar organizations.

Benchmarking is a process for identifying and importing practices to improve performance.

2 The Problem

How is 'Best Practices' used in the HIPAA context? If practices are not being benchmarked, is another term like 'common practice' more appropriate? Might common practices be more appropriate than best practices in some circumstances?

2.1 The Term

A search was performed from www.google.com for the keywords "HIPAA Best Practices" on Feb. 17, 2002 and retrieved the following 10 web sites as most relevant (for each site a brief description is provided):

1. www.himss.org "HIPAA Best Practices" by Tom Newton is a case study of one organization Carilion Health System and its approach to HIPAA. HIMSS is the Health Information Management and Systems Society.
2. www.rx2000.org has a section entitled "Tools and Best Practices" that sells four documents of which a typical example is: "HIPAA, A Provider's Perspective: Alan Abramson, CIO, HealthPartners, Minneapolis, MN from 4/26/2000". Abramson is sharing his experience. Rx2000 Institute is a member-supported healthcare technology organization.
3. www.ihaonline.org is a dead link for HIPAA Best Practices Forum of the Iowa Hospital Association. However, further study of the site finds reveals a discussion board that has a top-level entry for 'best practices' dated 02/23/01 that says: "What is your organization doing to get ready for HIPAA? Any policies or procedures you would be willing to share with your peers?" There have been zero replies between February 2001 and February 2002 to query.
4. www2.state.id.us reveals that the Idaho Dept. Health and Welfare has an emphasis on improvement that would be consistent with a concern for best practices.
5. www.nga.org points to the Centers for Medicare and Medicaid Services (CMS) online tool, called the HIPAA-Compliant Concept Model (MHCCM), to assist state agencies identify HIPAA best practices. From National Governors Association (NGA) Center for Best Practices.
6. another citation on Google's top ten is also from NGA Center for Best Practices and explains how eighteen states have unveiled websites to support HIPAA best practices.
7. www.hsciso.med.utah.edu points to a site entitled "Information Security Best Practices" but containing only "Sorry for the lack of content. This is currently being developed" from University of Utah Health Sciences Center
8. www.dmh.cahwnet.gov is the California Department of Health Services "HIPAA Toolkit: Best Practices" and points to five other web sites none of which systematically determines Best Practice.
9. enterprisesecurity.symantec.com is Symantec's HIPAA Integrated Security Service and says: "provides information security solutions that incorporate best-practices" but is not best practices in formal sense.
10. www.worldwebtalk.com advertises a "HIPAA Compliance: Best Practices and Q&A Live Webcast" hosted by WorldWebTalk.Com in which speakers present their practices.

The review of these 10 cites indicates that none reflect best practices in the strict sense.

2.2 Common Practices

While health care professionals with HIPAA responsibility want to know what practices are best, they may be far from that point. Hal Ahmens of Lyon, Popanz & Forester's Consulting said, "If an organization does something that may be useful to others, it would be presumptive to share it under a claim that it is a 'best practice'. At this point in the implementation of HIPAA, most of the organizations that we talk with are simply interested in practices that are working. " In circumstances like HIPAA, very little experience exists, and time is limited. If an organization has a practice that is effectively solving a problem, then others may like to know that practice. The practice need not be a 'best' practice. Another organization can decide whether to use the practice completely or to tailor it to fit.

Organizations entering the 'best practices' arena might instead begin with 'better practices' in small steps. To do this an organization should first look at

- similar organizations and
- simple processes.

Then on identifying a 'better practice', the organization would import it and sustain the practice. In trying to better the practice, an organization will gain experience with benchmarking. The sloppy approach generally taken to 'best practices' is a reflection in part of the absence of systematic benchmarking.

The first step is 'shared practice'. It implies only that the people doing the sharing have enough confidence in their practice that they are willing to have others look at the practice. If a number of people use this 'shared practice', then the practice would move to the status of a 'common practice'.

Are 'common practices' good? Robert Ken Kirch of KMPG says: "Because something is a common practice does not inherently make it a good practice. Most often, a common practice is dictated by factors other than the 'best', such as lack of resources, other priorities, or path of least resistance. For example, it may be common practice not to encrypt data on laptop computers even though the laptops may contain sensitive information. Another common practice is to never change passwords."

Can the industry first identify common practices and then select from those the good ones? Might a body of 'wise people' review what the market has produced, identify 'good practices', and publish them? Peter Haigh of Verizon has suggested that 'good practices' might lead to 'industry standards'. An 'industry standard' is 'a voluntary, industry-developed document that establishes requirements for products, practices, or operations.' These industry standards would complement the HIPAA standards by specifying in more detail entity types what would constitute 'good practices'.

2.3 When Common is Best

The X12 Transaction Standards are artifacts and not themselves an issue of best practice. However, the process for coming into compliance with the standard or the process for maintaining compliance once achieved are both processes that might be done better or worse and an organizations could learn from one another.

Likewise, the processes for coming into compliance and maintaining compliance with the Privacy Rule is a topic amenable to best practice analysis.

However, the Privacy Rule itself describes an under specified process and creates a special case not supported by best practice. The Rule specifically notes that different organizations may have different processes that would be compliant. For instance, a small group practice relying on paper records might implement the Minimum Necessary Process by simply having staff aware of the importance of confidentiality. However, an integrated delivery network with electronic records would be expected to implement access by role. Those entities of a kind that would be expected to have the same Minimum Necessary Process are not competing to have the best process. Rather they want to agree to a common process. This common process would represent the lowest common denominator of what would work. In this way, the entities would create a practical, de facto standard that the government would be compelled to recognize. If the like entities do not work together to produce this common practice, the process that is to be considered standard will need to be determined by the government with possibly adverse consequences to the entities. Thus, here one does *not want best practice but common practice*.

3 Taxonomy

One problem with trying to identify HIPAA common practices is the complex character of HIPAA compliance. HIPAA compliance might be seen along two dimensions, the Rules and the entities:

- The rules cover at the top level transactions, privacy, and various proposed rules,.
- What constitutes appropriate practice varies by the entity type and its approach to compliance.

Various kinds of artifacts and processes are impacted, such as policies and software systems.

3.1 Rules

Each Rule includes many parts, such as the 9 transactions of the Transactions Rule or the minimum necessary process and patient rights of the Privacy Rule. One breakdown of the Transactions and Privacy Rules follows:

Transactions
- insurance verification (270/271)
- authorizations (278)
- billing (837)
- follow-up (276/277)
- cash posting (835)

Privacy
- Consent and Authorize
- Uses and Disclosures
  - Minimum Necessary
  - Business Associates
  - De-identification
- Opportunities to Object (e.g. directory listing)
- Patient Rights
  - Access
  - Amend
  - Audit
- Administration
  - Documentation
  - Training
  - Security
  - Complaints
  - Sanctions

While the Final Rules are fixed pursuant to any official issuance of modification, different ways to categorize the rule components exist.

3.2 Entity Compliance and Type

The characteristics of a practice that will affect its appropriateness to be imported into another organization include its general features and its approach to compliance:

Entity Compliance
- Life Cycle
  - awareness
  - gap analysis
  - risk analysis
  - planning
  - training
  - implementation
  - audit
- Management
  - finance
  - human resources
  - operations

Entity Type
- Providers
  - Veterans Administration Health System
  - Department of Defense Health System
  - integrated delivery network
  - hospital network
  - academic medical center
  - small hospital
  - small group practice
  - independent laboratory
  - pharmacy
- Payer
  - Medicare
  - Medicaid
  - Blue Cross Blue Shield
  - Commercial payer
  - HMO
- Clearinghouse
- Vendors
- Consulting companies

The breakdown of entity compliance and type is not a fixed one. For instance, the life cycle of compliance may vary depending on the organization. The taxonomy could be refined to accommodate the various possible life cycles. The basics of any compliance life cycle are:

- education,
- implementation, and
- control.

One approach to exploring what is common is to analyze the published literature. The book *HIPAA Security* (Rada, 2001) is one source of published literature that addresses life cycle. That book provides several case studies that include descriptions of the life cycle used in pursuing HIPAA compliance, as follows:

Maryland General Hospital:
- awareness
- impact analysis
- planning for implementation and implementation
- training and enforcement
- audit

Providence Health System:
- formed project team
- asset inventory database
- policy and procedure development
- risk management assessment
- re-engineering

University Physicians Incorporated of Maryland:
- awareness and project team
- gap analysis
- planning
- implementation and audit.

These different life cycles are consistent with the life cycle offered in the taxonomy.

4 Practice Examples

A complete inventory of current practices is not practical to develop. However, a suggestion of the insights that might accrue from a systematic study of what is happening can be obtained from a partial inventory. A few differences will be identified among entity approaches as reflected in the published literature.

4.1 Finance

Practitioners appreciate a sense of what their peers are doing as reflected in surveys, as these surveys give a sense of what is common practice. One such survey (PHS, 2002) in the HIPAA realm is analyzed here for further insights along the line of both entity types and budgets.

The proportion of hospitals spending greater $300k per hospital to comply is directly proportional to size of hospital:

	2001			2002		
	small	med	large	small	med	large
<$300k	30	130	107	28	95	51
>$300k	0	4	27	0	23	76

As the number of beds of hospital increases, does the expenditure per bed decrease? Based on reasonable simplifying assumptions about the average expenditure and average bed size the following results:

average per bed expenditure in 2001		
small	medium	large
$3,000 per bed	$900 per bed	$300 per bed

The explanation for this difference may be as simple as economies of scale. The alternative explanation is that small hospitals are unnecessarily targeting the compliance standards of large entities, while the flexibility of the HIPAA rules would permit the smaller entities to face less difficult criteria. Small hospitals might together define their common practices as something less onerous than what large hospitals need to do. Based on other studies done by this author, the typical small group physician practice is spending next to nothing to date and is thus avoiding the problem of spending disproportionately more than larger practices.

4.2 Human Resource

By now, enough organizations have started their HIPAA compliance efforts that one can generalize about the organizational starting steps. In addition to obviously having an awareness effort, the larger organizations tend to form a multi-faceted HIPAA Committee. For small group physician practices, the office manager continues to assume all managerial responsibility for implementing compliance activities.

A case study of two integrated delivery systems, Carilion Health System and Children's Hospital of Wisconsin, revealed largely similar approaches (Rada et al, 2002). In January 2000, Carilion appointed its Information Security Officer as its HIPAA Project Team Leader. At Children's, serious consideration of HIPAA began in early 2000, with the hiring of an Information Security Officer who worked with the organization's Compliance Director to initiate its HIPAA Project. In both cases, early 2000 marked the start of formal HIPAA efforts, the leadership came from the information systems unit of the entity, and the HIPAA Project Team Leader reports to the CIO.

The membership of the HIPAA Project Team represents those units of the entity most impacted by HIPAA. For Children's Hospital of Wisconsin, the units represented on the Project Team include:

- Administration,
- Information Systems,
- Finance,
- Legal,
- Compliance,
- Inpatient,
- Ambulatory,
- Satellite Services,
- Medical Records, and
- Quality Improvement.

The HIPAA Project Team is divided itself into sub-teams to address Transactions and Code Sets, Identifiers, Privacy, and Security. The composition of the HIPAA Project Team is similar across large provider organizations. For instance, the University of Utah Health Science Center has a Privacy and Security HIPAA Committee with about 25 people from the major components of the Health Science Center with a particular emphasis on those roles related to systems and compliance, as is the case at Carilion and Children's.

The breakdown of the HIPAA Project Team at Carilion included one sub-team not explicitly identified at Children's. This extra sub-team is called the 'Corporate Sub-team'. The Corporate sub-team addresses training, public relations, and legal issues. The topics addressed by the 'Corporate Sub-Team' are also addressed at Children's but not within a separate sub-team. This difference might relate to Carilion being larger and more diverse in functions.

Another issue is the reporting structure of the HIPAA Project Team within the entity. Typically, the project team might report to a steering committee, as illustrated here:

- NYU Medical Center has an organizational structure that begins with a Executive Steering Committee composed of the Vice-President for Health Affairs and the General Counsel. The HIPAA Working Group is

chaired by the CIO and breaks into functional teams based on the phase of compliance, such as a team for gap analysis.

- The Idaho Department of Health and Welfare had separate HIPAA projects for different rules. To bring the enterprise perspective to this project, the management of the project was transferred to the joint executive sponsorship of Information Technology and Management Services. The project has combined the requirements related to codes and transactions, privacy, security, provider identifiers and national identifiers into a single enterprise project

Some entities focus the specification of their Committee composition on the different parts of the HIPAA rules that need to be addressed. Some focus on the functional decomposition in the entity. Without evidence of the impact on performance or compliance of the various approaches to the staffing of the HIPAA team, one cannot say what is a best practice or not but only what is a common practice.

These reviews of the composition of an entity's HIPAA Committee have not directly addressed issues such as the culture of the organization and its commitment to compliance. Reflected in the organization and staffing of the HIPAA Committee will be an entity's commitment to HIPAA compliance. An example of an organization seemingly committing at the top level to HIPAA compliance comes in the this quote from the Idaho Department of Health: "HIPAA provides the impetus for us to align our work practices, thereby improving our service delivery to the public." For some organizations, the vision is different and HIPAA is only a compliance issue. How organizations will staff and structure their HIPAA teams will reflect their commitment.

5 Tools Examples

The practices for HIPAA compliance focus on the activities of people. People often use tools to support their activities, and such tools merit analysis for what is common in HIPAA compliance. This section examines briefly operations, transactions, and training. For every rule component and every phase of compliance there could be a section about the tools that support it. As one might expect, the simpler tools seem the more widely used.

5.1 Operations

Numerous tools have been developed to support entities in complex processes. However, the typical problem with their adoption is the need for all participating users to become trained in the specialized tool, to enter data into it, and to update it. Given these difficulties, even the largest entities may find themselves preferring simple, non-specialist tools to support project management.

One of the most popular of the non-specialist project management tools is Microsoft Project. Some Microsoft Project templates are publicly available that give the life cycle of compliance in great detail along with time periods, deliverables, and resource requirements (see Figure "MS Project HIPAA Plan"). These Microsoft Project templates might be modified to suit a particular entity's needs.

5.2 Transactions

Small group physician practices tend to rely on third party administrators, clearinghouses, or vendors for support of their provider-payer transactions and for compliance with the HIPAA Transactions Rule. Larger entities have often done some work toward analyzing the gap in their internal formats and what HIPAA expects. Tables are available that give the details of a X12 Transaction Implementation Guide and facilitate an entity mapping non-standard formats with what is required for the standard.

The popularity of these X12 gap analysis tables is indicated by their wide availability. For instance, the Association for Electronic Health Care Transactions has posted two tables that provide a 'content gap analysis' between HCFA 1450 and HIPAA 837I and between HCFA 1500 and HIPAA 837P. Each table provides a crosswalk between the HCFA paper claim format and the HIPAA compliant Implementation Guide. Each table also identifies critical data content gaps.

Having determined the gaps, an entity may need to change some of its internal data collection or analysis processes.

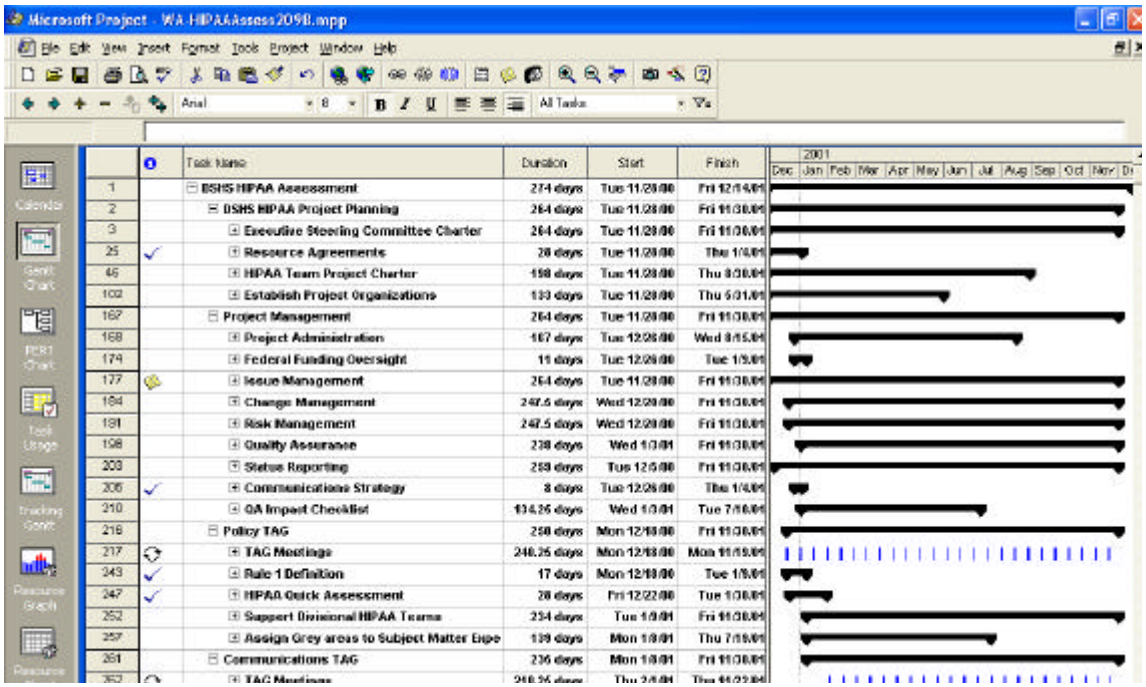

Figure "MS Project HIPAA Plan": This screen shot of a Microsoft Project HIPAA work plan comes from the State of Washington Department of Social and Health Services. The entries with pluses can be selected and then unfold to reveal further detail.

Additionally, the entity has to decide whether it relies on its vendors and clearinghouses to do the mappings that are needed to relate any of its non-standard formats to the standard or not. If not, then the entity must either change its internal processes or acquire and deploy a mapper (Rada, 2002).

Numerous commercial mappers exist. Some of the best-known mappers are from Mercator, Sybase, WebMD, and Microsoft. The solutions typically include predefined definitions and data maps for the X12N Version 4010 standards, as well as for HL7, UB92, and NSF formats. The mappers can be used to integrate applications, interfaces, and data resources across the enterprise. They typically include tabular forms for specifying the relationships between two forms (see Figure "Specifying the Filter") and various graphical interfaces for defining connections to different sources of data.

Using the mapper does not mark the end of the challenges to compliance. One problem is the coordination of testing across the many entities that exchange transactions. WEDI-SNIP has been helping share information germane to this coordination of schedules.

5.3 Privacy Training

Training can either be developed in-house or acquired from the outside. Carilion Health System has developed its own videos because it prefers the product to be completely tailored to the specifics of Carilion. For those entities that consider to acquire training from elsewhere, the range of options is multiple:

- hcPro is a healthcare publishing and training company that provides paper, online, and video training for HIPAA. Paper products include a 40-page privacy brochure that comes in different versions depending on the targeted staff.

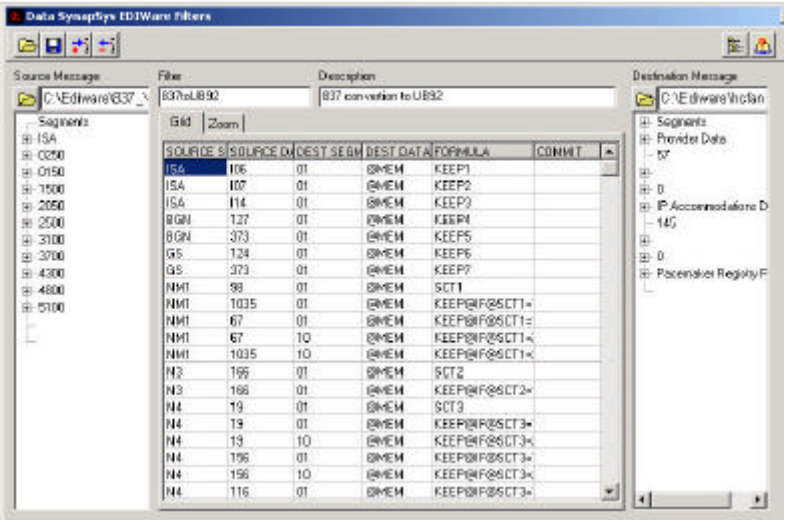

Figure "Specifying the Filter": In this screen the mapping from a field of the HIPAA 837 to a field of the UB92 is defined. The user could also through entries in this table modify the mapping and implement a mapping from any one form to any other form.

- Some big consulting companies have solo or in partnership offered training programs that emphasize the management of employees through the training system. For instance, Ernst & Young has an alliance with the medical publisher CCH to offer enterprise-oriented training through a web portal.
- Some big consulting companies focus their educational efforts on awareness training aimed to convince executives of the need to take action on HIPAA rather than HIPAA training for the entire workforce.
- Several professional societies, including AHIMA and HIMSS, offer HIPAA training and are introducing HIPAA certification programs too. This raises yet another interesting issue of the extent to which the employer or some outside entity will certify training on HIPAA.

This analysis suggests yet another dimension to the taxonomy -- namely, the range of non-covered entities that service health care entities.

6 Paths to Sharing

Sharing is occurring. The sharing work of WEDI-SNIP, the State Health Departments, and the academic medical centers is particularly prominent. Yet, this spirit of sharing is not universal. A senior officer at one Maryland multi-hospital integrated delivery network explained:

- Everyone must achieve HIPAA compliance.
- Accordingly, being HIPAA compliant is not a competitive advantage.
- One may have a competitive advantage for how one has cost-effectively developed HIPAA compliant programs, and thus one would not want to share this.

A senior officer from HCA had a different reason for not wanting to share HIPAA practices. HCA's rationale was that such sharing might make the entity more susceptible to lawsuits.

Consultants and vendors provide some useful information free. However, generally they are in the business of selling their understanding of good practices and tend to constrain what they make available free.

Government might take the lead in developing public repositories of 'good practices'. The Administrative Simplification Compliance Act invites covered entities to submit plans for compliance with the Transactions Rule. Furthermore, it states:

> "The Secretary of Health and Human Services shall furnish the National Committee on Vital and Health Statistics (NCVHS) with a sample of the plans submitted ... NCVHS shall analyze the sample of the plans furnished. NCVHS shall regularly publish, and widely disseminate to the public, reports containing effective solutions to compliance problems. Such reports shall not relate specifically to any one plan but shall be written for the purpose of assisting the maximum number of persons to come into compliance by addressing the most common or challenging problems encountered."

NCVHS is in a good position to help create and publish 'good practices'. Two caveats are in order:

- What will constitute good practice for one type of entity, like a solo-physician practice, is likely to be different from what will constitute good practice for a 50-hospital network. 'Good practices' may need to be identified by entity-type.
- The value of a repository of good practices will be high, if and only if, the repository is readily accessible and is properly maintained across time.

If these two caveats are observed, then the resulting 'good practices' will be valuable to covered entities.

Increasingly, toolkits for HIPAA compliance, replete with 'good practices', may become widely, inexpensively available from government, professional societies, and others. Those responsible for implementing HIPAA compliance programs will then be able to focus on the changes needed inside their organizations rather than on re-developing the toolkits that are common across like-entities.

Collecting and sharing experiences is a goal in different contexts. For instance, the American military has tried for decades to foster software reuse. The military has tried to build libraries of reusable software into which its contractors would deposit software objects that could be reused by subsequent contractors. This effort has failed in part due to the rapidly changing character of software objects. In the realm of HIPAA policy documents, the rate of change might be relatively slow.

Another challenge to reuse and benchmarking is that organizations are often not motivated to share their practices. Even in a relatively constrained domain such as state Medicaid agencies, the challenges of dealing with the range of the HIPAA rules and the phases of compliance are many. Nevertheless, CMS has provided an extensive roadmap. Will this roadmap be extended and provide a reliable resource for the states. Some of the expertise is not native to CMS or the states. Perhaps other entities like the National Library of Medicine could also contribute to supporting the maintenance of the taxonomy and the collection and indexing of documents. The National Governor's Association might help, as might a wider alliance of organizations.

The challenges to Medicaid agencies are different from those to providers. Another government entity that might be motivated to support the sharing of HIPAA practices is the Veterans Administration. The VA maintains a 170-hospital network and might share experiences across that network and with the wider public.

7 Conclusion

Managers want 'best practices', and in the media any respected organization's approach to HIPAA compliance tends to be treated as though it were an established 'best practice'. However, this common use of the term belies the importance of addressing 'best practice' in a rigorous fashion and understanding the differences between 'best practice', 'good practice', and 'common practice'. Best practice is a process that is quantifiably successful over time and must be transferable to similar organizations. Common practice occurs frequently.

As the HIPAA Privacy Rule emphasizes flexibility by entity-type, these entities have an obligation to be pro-active in sharing experiences and identifying common practices. These common practices might effectively define what constitutes adequate compliance. The example of how small hospitals are paying ten times more per-bed to achieve

HIPAA compliance than are large hospitals is one possible indicator of the failure in the market of the small hospitals to establish their common practices as simpler than those of the large hospitals.

Establishing common practices, let alone best practices, is not something that one committee can accomplish by deep thought. Rather entities should contribute documentation of their current practices to appropriate libraries. There the documents would be indexed, organized, and analyzed. This indexing would be done with terms from a taxonomy such as that sketched in this manuscript. The taxonomy has at its root two concepts of 'rules' and 'entity compliance and type'.

As one begins to build these libraries by collecting documents from colleagues or public sources, one realizes how readily the information can be reused. Examples of the insights and resources readily discovered include:

- The staffing of HIPAA project teams and scheduling their work will vary from entity to entity and across the phases of compliance but according to certain patterns. The HIPAA project team for privacy will tend to have representatives from every functional unit of the entity with an emphasis on systems staff.
- While sophisticated, legacy tools for enterprise-management can be applied to managing the HIPAA project team, simple templates from Microsoft Project have been diffusing in the market. These Microsoft Project templates are easy to use and modify.
- The transactions gap analysis is typically done with tables. Each table covers a specific X12 transaction and comes prepared with those X12 transaction details. The entity enters information into the blanks of the table to specify differences between the X12 requirement and the format currently employed by the entity. From such a gap analysis, parameters of a mapper can be readily set so as to automatically translate transactions from one format to another.
- Different vendors offer different types of privacy training. The analysis of the training options reveals the value of extending the taxonomy to address vendor types as well as covered entity types.

Clearly, documented, common practices can help an entity cost-effectively achieve HIPAA compliance.

Some libraries of reusable HIPAA practices will be maintained by the government and made freely available to the public. Some libraries of reusable HIPAA practices are only accessible to those who pay a fee, and the fee, in turn, pays those who maintain the library. Government-funded health care entities should be at the forefront of publicly demonstrating their libraries of HIPAA practice. The state Medicaid agencies have made a step in this direction, as have the academic medical centers. The effort needs to be continued and to be joined by others, such as the Veterans Health Administration.

Opportunities for sharing documentation of HIPAA practices exist. However, without coordination, these efforts to share are under-appreciated. Successful coordination is built on a common language that should include an operational definition of best practices and a taxonomy of the domain of practices. The collected documents need to be organized and appropriate access provided. Covered entities should be able to readily find and use the documents relevant to their needs.

8 References

PHS (2002) "U.S. Healthcare Industry Quarterly HIPAA Compliance Survey Results: Winter 2001-2002" Phoenix Health Systems (PHS) and Healthcare Information and Management Systems Society (HIMSS) available from www.hipaadvisory.com.

Keehley, Patricia, Steven Medlin, Sue MacBride, and Laura Longmire (1997) *Benchmarking for Best Practices in the Public Sector*, Jossey-Bass Publishers: San Francisco.

Rada, Roy editor (2001) *HIPAA Security: from the Proceedings of the 2001 Annual HIMSS Conference*, published by HIMSS, October 2001.

Rada, Roy (2002) "Transaction Efficiencies" *HIPAA@IT Monthly Update*, January 2002, available from www.hipaa-it.com.

Rada, Roy, Chuck Klawans, and Tom Newton (2002) "Comparing HIPAA Practices" *Journal of Health Information Management*, Spring 2002.