Policy Analysis Brief

March 2004
W Series • No. 3

NORC | WALSH CENTER FOR RURAL HEALTH ANALYSIS

Rural Hospitals' Strategies for Achieving Compliance with HIPAA Privacy Requirements

The Health Insurance Portability and Accountability Act (HIPAA) directed the Department of Health and Human Services (DHHS) to adopt uniform national standards to protect the confidentiality of health information. HIPAA requires hospitals and other covered entities to take steps to safeguard against the misuse of individually identifiable health information and to limit the sharing of this information. Health care consumers are granted rights to control how their health information is being used and disclosed. To ensure that the privacy rule does not impose an undue burden on these small providers that may not need and/or cannot support complex procedures, DHHS premised the privacy rule on the concept of *scalability*. Scalability refers to the expectation that covered entities implement privacy procedures that are appropriate to the organization's size, available resources, existing technology and organizational needs. Thus, while standards are uniform, hospitals have flexibility to adopt privacy procedures that are appropriate for their individual circumstances.

Hospital Responsibility under HIPAA Privacy Rule

Privacy Procedures & Notice of Privacy Rights: *Develop privacy procedures; notify patients of privacy rights and of how protected health information (PHI) is used*

Minimum Necessary: *Disclosures of PHI limited to that minimally necessary to achieve task*

Authorization: *Obtain patient permission to disclose PHI for purposes other than treatment, payment, & certain health operations*

Safeguards: *Administrative, technical and physical safeguards of PHI must be in place*

Business Associates: *Enter into arrangements with business associates that ensure protection of PHI*

Privacy Officer: *Designate person responsible for development & adherence of privacy policies*

Training: *Provide staff with privacy training*

In the Fall of 2002 and the Winter of 2003, the Walsh Center for Rural Health Analysis interviewed administrators from rural hospitals throughout the U.S. to gather information on the strategies that they are using to ensure that their facility complies with HIPAA privacy standards.

Hospitals were selected to participate in this study if, as suggested by responses to a HIPAA

readiness survey, their privacy policies and procedures were in the process of being implemented or were already in operation. Eight hospitals were chosen for in-depth telephone interviews. These hospitals were chosen to achieve geographic diversity and to include facilities with special rural designations — Sole Community Hospitals, Critical Access Hospitals and Rural Referral Centers. Persons interviewed included Chief Executive Officers, Privacy Officers, Corporate Compliance Officers, and other administrators.

This brief describes the key findings from these case studies.

Key Findings:

Who do rural hospitals select to serve as the privacy officer?

Hospitals implemented several of the compliance strategies suggested by the HHS in their guidance documents, including assigning privacy officer responsibilities on a "part-time" basis to an employee with related duties.[1] Many of the hospitals that we contacted had delegated the responsibilities of privacy officer to the medical records manager or information systems manager. Only one hospital hired a dedicated full-time privacy officer. Although rural hospitals rarely hired support staff to assist the privacy officer in the performance of duties, several hospitals had established task forces or internal committees to assist the privacy officer with interpreting rules, developing policies and training staff.

Scalability of HIPAA Privacy Standards

"The privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan. For this reason, we propose the privacy principles and standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity. We intend that implementation of these standards be flexible and scalable, to account for the nature of each covered entity's business, as well as the covered entity's size and resources…, we would require that each covered entity assess its own needs and devise and implement privacy policies appropriate to its size, its information practices, and its business requirements."

Federal Register, 1999. *Proposed Standards for Privacy and Individually Identifiable Information.* 64 (212): 59925.

How do rural hospitals train employees on privacy standards?

All hospital representatives interviewed for this study emphasized the importance of staff education for the success of their privacy programs. Indeed, the privacy rule requires that a hospital train its workforce on privacy policies and procedures. Where hospitals differed was in the type of training that was used. Some hospitals were using traditional "classroom" style lectures combined with post-testing, while other hospitals were relying on self-directed approaches that include training manuals and computer-based training modules. A number of hospitals indicated that following the initial training, on-going education was provided through regularly scheduled lectures and articles in their employee newsletters.

On a related note, hospitals recognized that the new privacy policies and procedures may inconvenience or confuse members of the community. As a way to educate the public on the reasons for and the nature of the changes in hospital procedures, some hospitals placed information about their privacy programs in local newspapers and on the facility's website.

All hospitals had either developed or were in the process of developing policies for sanctioning employees who breach patient privacy. Often sanctions were scaled to reflect the severity of the offense. For example, one hospital administrator indicated that if a breach occurred by accident or because of curiosity, such as when an employee reviews a patient's medical record to look up their birth date, the employee generally receives counseling on the violation. A breach conducted for personal gain, such as an employee using information in medical records to identify potential private-duty nursing clients, results in a written warning. A gross infraction, such as one that results in significant personal gain and causes

1 Office of Civil Rights, Department of Health and Human Services. *Standards for Privacy of Individually Identifiable Information.* December 4, 2002. http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf

embarrassment to the patient and or hospital, results in termination.

What strategies are rural hospitals using to protect patient privacy?

Rural hospitals are implementing a variety of low-cost strategies to safeguard patient privacy and prevent against inappropriate disclosures of health information. Electronic restrictions, such as the use of passwords, personal identification numbers or other access codes, were among the most frequently cited safeguards. Cipher, combination and keyed locks were also commonly used to restrict access to medical records, transcription rooms, or any other protected materials. The following are examples of other approaches that are being used to protect patient information:

- One hospital routinely used a "white board" to list each patient on the floor and the specific treatment that they were receiving. Prior to implementing privacy procedures the board was located in a corridor where it was readily visible to anyone walking past the area. This board was simply moved behind a door that could not be accessed by persons outside the department.
- At another hospital, the room where physicians reviewed patient x-rays overlooked the main entrance to the hospital. At night, if the blinds were not closed, anyone entering the hospital could very clearly see the films on the view box. Although the patients' name could not be read from this distance, the hospital still considered it an inappropriate disclosure. The hospital implemented a policy that required blinds in the room to be drawn at night.
- One hospital implemented a new patient registration protocol in an effort to make the process more private. Under the former registration system patients would stand in a line at the reception desk waiting to provide their personal information. Under the new system, each patient receives a number upon arrival at the hospital and only when the patient's number is called are they asked to approach the desk.
- A few hospitals had established policies for faxing patient information. At one hospital dedicated fax machines are used to handle routine department-specific procedures, such as transmission of lab results. To ensure an even greater level of privacy, medical records can only be faxed to a specifically named recipient (as opposed to a department name) and must contain a cover sheet. Another hospital updated all its thermal based fax machines because this fax technology created a faint negative from which information could be read.

What are the costs associated with compliance?

Several hospitals provided information on the costs of implementing selected aspects of the privacy rule but we were generally unable to determine the total costs incurred. In some instances hospitals had either not estimated these costs or could not separate the costs spent on implementing privacy standards from the cost of implementing other HIPAA standards (e.g., transaction or security). Although several hospitals expressed substantial concern over the compliance costs, at least two of the hospital representatives that were interviewed for this study indicated that HIPAA did not pose a significant financial burden. It is important to note that all hospitals that were eligible had applied for and received a Small Rural Hospital Improvement Grant Program (SHIP) grant; SHIP funds may be used to pay for HIPAA-related costs, including the purchase of technical assistance, training services, and information technology.[2]

Rural hospitals represented in these case studies also cited numerous strategies to mitigate the time and financial resources needed to achieve compliance with the privacy standards. Hospitals that were part of a larger system or that were affiliated with a hospital association were often able to take advantage of these relationships to manage compliance costs. Hospitals often customized the policies and procedures developed by the parent organization or an affiliated hospital instead of developing them from scratch. Several hospitals, whether or not they were a part of a larger system, were using relatively inexpensive training tools (e.g., booklets, videotapes) that were purchased from regional hospital consortia or trade associations.

[2] SHIP grants are available on a non-competitive basis to short-term, general acute care hospitals with 49 beds or less that are located outside a metropolitan statistical area (or in a rural census tract of a metropolitan statistical area). Awards approximate $10,000 and, in addition to HIPAA-related activities, may be used to pay for costs associated with implementation of the prospective payment system, and to support quality improvement activities.

Conclusions

Rural hospitals in this study recognized the importance of ensuring the confidentiality of patient health information and have made substantial progress in achieving compliance with HIPAA privacy standards. Although these rural hospitals were using the flexibility afforded to them under HIPAA to develop common-sense approaches for promoting patient privacy, each of the rural administrators interviewed acknowledged that additional work will be required to effectively secure patient privacy, particularly as technology and the need for information advance. Organizations charged with ensuring HIPAA compliance or trade associations that represent rural hospitals should continue to identify gaps in knowledge and to assist rural providers in identifying effective, low-cost compliance strategies.

This study was funded under a cooperative agreement with the federal Office of Rural Health Policy (ORHP), Health Resources and Services Administration, DHHS (U1CRH00026-04-00). The conclusions and opinions expressed in this report are the authors' alone; no endorsement by NORC, ORHP, or other sources of information is intended or should be inferred.

The Walsh Center is part of the Department of Health Survey, Program, and Policy Research, NORC, a national organization for research at the University of Chicago. To obtain a copy of the full report or for more information about the Walsh Center and its publications, please contact:

NORC Walsh Center for Rural Health Analysis, *7500 Old Georgetown Road, Suite 620, Bethesda, MD 20814-6133.*
(tel) 301-951-5070.
(fax)301-951-5082.
www.norc.org

7500 Old Georgetown Road, Suite 620, Bethesda, MD 20814-6133

NORC | WALSH CENTER FOR RURAL HEALTH ANALYSIS