HCCA HEALTH CARE COMPLIANCE ASSOCIATION

# Compliance TODAY

November 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

## The Evolution of Healthcare Law and Compliance

**an interview with Sara Kay Wheeler**
**2015–2016 SCCE/HCCA Board President**
**Partner, King & Spalding**

*See page* 16

by Michelle C. Evans, MPA, CHC, CHPC and Kenneth A. DeVille, PhD, JD

# HIPAA Privacy walkthroughs: The convergence of policy, education, and monitoring

» HIPAA Privacy "walkthroughs" are a proactive means of supporting the elements of an effective compliance program.

» Annual HIPAA walkthroughs are a potential means of identifying HIPAA violations and departures from regulations and can enhance training.

» Checklists should focus on the issues that are of greatest risk and regulatory concern for the particular clinic setting.

» Announced, "no fault" visits emphasize that walkthroughs are primarily a collaborative process.

» Post-walkthrough reports should include specific directions on regulatory requirements as well best practice recommendations.

***Michelle C. Evans*** *(evansmi@ecu.edu) is Director, Office of Institutional Integrity/ECU HIPAA Security Officer and* ***Kenneth A. DeVille*** *(devillek@ecu.edu) is Chief Institutional Integrity Officer/HIPAA Privacy Officer at East Carolina University in Greenville, NC.*

Compliance departments and compliance officers often struggle with the multifaceted yet interlocking nature of their mission. They must understand and communicate the technical and sometimes nuanced requirements of applicable state and federal regulations. They must develop institution and practice-specific policies that support and promote compliance with those regulations. Institutional actors from leadership, middle management, and providers, to operational staff must be educated on these regulations and policies. But mere education on regulatory requirements and policies is insufficient.

The concrete, day-to-day implications of regulations and policies must be communicated to leadership, staff, and providers in such a way that they can be applied in real-life practice settings. Employees must understand how policies and regulations apply in *their* work settings. This mandate can be especially challenging in larger medical centers and practices in which there are frequently multiple, even dozens of, individual clinics, offices, and departments in which the range of work flows may present an array of different compliance challenges. Finally, the existence of policies and formal education on those policies is insufficient if employees do not follow established standards and guidance. Compliance officers are responsible for monitoring adherence to applicable policies across varying practice settings and taking corrective action where appropriate.[1] All of these goals must be addressed in a context of limited human and financial compliance resources.

Evans

DeVille

Regular HIPAA Privacy "walkthroughs," or "walking rounds," are a recognized means of effectively and efficiently protecting patients, supporting the elements of an effective compliance program, and helping

ensure adherence to HIPAA Privacy standards.[2] HIPAA Privacy walkthroughs require, in one sense, little more than a compliance officer physically touring clinics, offices, and departments and evaluating the various facilities and work sites, observing work flows, and talking to staff and providers. Ideally, the compliance reviewer will refer to a prepared checklist identifying key regulatory requirements, institutional policy directives, and recommended guidance and confirm by observation and interviews whether those concerns are addressed in everyday, real-life practice. HIPAA walkthroughs are a potential means of identifying HIPAA violations and departures from regulations. But a carefully structured and appropriately executed program can yield additional, and perhaps far more important, benefits that justify and exceed the resources required to conduct them on a regular basis.

## First steps

Different covered entities will have a varying range of clinic and office settings, but the basic approach to initiating a walkthrough program is likely to look relatively similar. The authors serve an institution that treats patients in approximately 40 to 50 different clinics and practice settings. Walkthroughs may also be conducted in other non-clinic settings (e.g., financial service offices) that handle or process protected health information (PHI). But the essential features of a walkthrough program will be comparable in varying types of covered entities, even if the treatment settings are not.

The first step in initiating an ongoing walkthrough program should be the development of a checklist that will allow observation of staff and provide those who work in clinics with applicable regulatory, policy, and best practice guidance. The existence of the checklist is important early in the process, because it aids the Compliance or Privacy Office's review by focusing its goals and developing the most effective approach and strategies in conducting the actual walkthroughs. The development of a checklist as a first step will also allow others in the institution to understand more fully the nature of the exercise before it is launched.

## The walkthrough checklist

The development of a checklist to guide the HIPAA walkthroughs is a relatively straightforward exercise. The checklist should contain practice-related references to regulatory requirements, key institutional policies, and specific concerns related to the organization and medical work of the clinics that will be reviewed. Although walkthroughs are designed primarily as a means of evaluating risks and compliance with privacy concerns, there is also an opportunity to include scrutiny of many important HIPAA Security risks as well. A HIPAA Compliance Office can easily produce its own "home grown" checklist from scratch, but there are numerous model checklists available from various organizations and many academic healthcare centers that can be adapted for use.

The checklist can be formatted in any number of ways. But, it is useful to create a spreadsheet that includes the specific privacy or security concern or activity, an indication whether or not the expectation is met by the clinic's organization and practices, and a space for observations and recommendations by the compliance reviewer for follow up, if any is required. The checklist developed and employed by the authors contains approximately 70 items for inspection and scrutiny, but a workable checklist could contain either more or less depending on need and/or the risks of the institution. The categories and subject matter should focus on the issues, practices, and requirements that are of greatest

risk and regulatory concern for the particular clinic settings.

General walkthrough checklist topic areas might include:

- Information regarding the HIPAA Privacy Office
- Notice of Privacy Practices
- Exchange of PHI
- Physical inspection
- Printers, copies, and fax machines
- Computers and workstations
- Personnel issues
- Privacy procedures and workflows
- Mail
- Disposal of PHI

The checklist should include an evaluation of specific clinical practices under each general subject area. For example, clinic employees should understand the role of the Privacy Office, know how to contact it for questions and concerns, and report privacy concerns to a manager or privacy officer as appropriate. Do employees know where to reference institutional HIPAA policies? Are employees correctly using authorization forms or directing PHI requests to the Release Office? Walkthroughs are also an excellent opportunity to evaluate the requirements related to the Notice of Privacy Practices (NPPs). Are NPPs posted in all clinical registration areas, and are English, Spanish, or other translated copies made available as needed? Do employees understand the contents of the NPP, and are NPPs collected and signed by patients as regulations require?

Walkthrough interviews present an opportunity to determine if employees understand the importance of exchanging only that PHI which is "minimally necessary." Visual observations and interviews help determine if employees protect patient privacy when interacting with patients and other staff. Telephone protocols and practices can be scrutinized. Physical inspection of the premises can provide broad insight into the protection of patient privacy and security. Is PHI kept in locked cabinets and behind secured doors when appropriate? How are whiteboards employed? Are employee desks cleared of PHI when unattended? Are printers, copiers, and fax machines in secure areas? Does the clinic have and follow appropriate protocols when using printers, copiers, fax machines, and receiving and sending mail? Important personnel and security issues might include the wearing of required ID badges, the appropriate use of passwords, and appropriate workstation practices. Is PHI disposed of in properly authorized ways? Is PHI placed in trash cans? Are locked shred bins available? Is electronic PHI properly destroyed? All such inquiries are important indicators of whether the clinic and its employees are appropriately protecting patient privacy.

### Notifying leadership and middle management

After the development of the walkthrough checklist, we advise the early engagement of as many institutional contacts as possible in preparing a walkthrough program. Depending on the institutional structure, the board of directors, deans, department chairs, the director of Nursing, the head of Clinical Financial Services, and/or other individuals in leadership should be informed of the project and its goals. Notifying leadership may not be necessary, but rather it ensures that they are not taken by surprise by the activities. Moreover, early buy-in and support from leadership will help blunt potential resistance and enhance cooperation from middle management staff and providers when they learn of the walkthrough program. In large institutions, leadership can identify the appropriate middle management contacts who may likely offer beneficial suggestions that may enhance the effectiveness of the project. This may also

help build support and trust, or allay fears, when the walkthroughs are initiated. In addition, notification to middle management can help mute resistance and enhance cooperation with the walkthroughs at the clinic level, if any issues materialize. The ultimate goal, however, is that transparency and prior notice will encourage staff and providers to view the exercise as a collaborative learning process, rather than a top-down, confrontational investigation.

In some institutions, it might be advantageous to present the planned walkthrough program to select committees for their information and input. The preliminary plans for the project might be outlined for nursing leadership committees, physician practice committees, patient services committees, clinical services committees, or other groups that may play a central role in the operational aspects of the practice or institution.

At the authors' institution, the project was forecasted at the HIPAA steering committee. Although the HIPAA steering committee typically focuses on policy-level decisions and guidance, committee discussion of the walkthrough program provided a means of further publicizing the activity in the institution. As importantly, it helped illustrate for the committee how policy issues are translated to the operational setting and underscore the committee's understanding of the work of the Privacy compliance team.

## Engaging staff at the clinic level

The authors recommend that the inaugural walkthrough visits are scheduled in advance and that the clinic personnel know specifically what practices will be scrutinized and evaluated. It is also advisable that the initial walkthrough visits are clearly designated as "no fault," educational exercises. There are obvious disadvantages to announced/no-fault walkthroughs. Such visits are clearly not true monitoring exercises. Clinic personnel, if they choose, have ample notice to use the checklist to prepare their clinics for the walkthrough and might revert to previous unwise and inappropriate practices once the walkthroughs have been completed. Our experience, however, suggests that this is not ordinarily the case.

Announced/no fault walkthroughs highlight the educational and collaborative component of the exercise.

But the advantages of the "no fault" approach, especially on the inaugural round of walkthroughs, are substantial. The goal of Privacy walkthroughs is not only monitoring; it is also communication and education. Announced/no fault walkthroughs highlight the educational and collaborative component of the exercise. One of the key advantages of a walkthrough is that clinic staff who have been exposed to only formal HIPAA education can now receive clinic-specific operational advice and insight. Clinic staff can see explicitly how the sometimes abstract and formal regulations and policies have a real-life, clinical component. Announced/no fault visits are more likely to enhance transparent communication between compliance staff and clinic staff and providers. Clinic staff are more forthcoming with answers and are more likely to ask questions when there is a collaborative trust established.

## Walkthroughs: Round one

The actual walkthrough should consist of one or two Privacy compliance personnel touring a clinic facility with one or two clinic managers.

This approach allows very concrete discussions about the contents of the walkthrough checklist and potential brainstorming on operational alternatives that would better meet regulations and protect patient privacy. These conversations, which sometimes occur during the walkthrough itself, create the opportunity to discuss such issues as the finer points of incidental disclosures or the appropriate way to balance operational convenience against enhanced patient privacy protections. Brief post walkthrough meetings invariably provide additional opportunities for HIPAA questions, concerns, and ideas from clinic management staff, both related and unrelated to the content of the walkthrough itself. Also, these post walkthrough debriefings allow compliance personnel to reinforce the philosophy and tenor of the exercise.

Following the post-walkthrough debriefings, the Privacy Office should provide email or hardcopy reports to the nurse managers and patient access managers, or whoever directly participated in the process, to outline the areas of concern, if any. Telephonic, written, or onsite follow-up may be appropriate, depending on the nature of the issue. These summary reports should include recommendations on specific regulatory requirements (e.g., posting of institutional NPPs) and best practice recommendations that would decrease the risk of breaches of patient PHI (e.g., improved workstation placement). Failure to meet explicit regulatory provisions (e.g., failure to post the NPP) should always generate high-priority follow-up inquiries to ensure that the clinic makes the necessary changes in a timely fashion. In contrast, best practice recommendations may be viewed as an ideal goal and revisited in subsequent discussions and walkthroughs.

> …best practice recommendations may be viewed as an ideal goal and revisited in subsequent discussions and walkthroughs.

### Annual walkthroughs: Round two and beyond

Walkthroughs *can* be designed as a type of one-time gap analysis in which institutional needs are assessed and remedied. However, we believe the walkthrough mechanism should be repeated at least annually in order to facilitate ongoing education and dialogue. Although launching the walkthrough program involves a significant expenditure of effort and compliance staff time in Year 1, subsequent iterations of the clinic visits will be less burdensome. Annual repeat walkthroughs as an established component of the Privacy Office's ongoing compliance program will allow the exploration of new issues and expose new staff and new workflows to the reviews.

Our experience with repeat annual walkthroughs has been gratifying. Most clinic managers were familiar with the process and the issues illustrated on the checklist from previous years. Fewer issues of concern were identified on follow-up visits, even a year hence.

As the Privacy Office's face-to-face contact with clinic employees has increased, so has its understanding and appreciation for wide range of clinical workflows, many of which are unique to a clinic or practice. This concrete understanding has aided the office in generating additional best practice recommendations, improved consultations,

and highlighted those situations that call for a new or revised institutional policy. The results of the HIPAA walkthroughs have also provided insight to the Privacy Office on the ways in which the new employee and annual HIPAA training can be enhanced and improved. Moreover, intimate knowledge of clinic workflows, gained from the walkthrough experience, has helped Privacy Office staff understand and unravel potential violation issues entirely unrelated to the walkthrough program. Many of the clinical staff recognized the compliance reviewers. The familiarity with the compliance staff, born of the walkthrough reviews, has led to many inquiries throughout the year to the Privacy Office, queries that may not have been made otherwise. Compliance officers everywhere seek to make all employees part of the compliance team—to make compliance everyone's business. Walkthrough programs can advance that goal.

It may be useful to escalate the scrutiny of the reviews as a walkthrough program evolves from year to year. For example, the walkthroughs conducted in Year 2 of the process could be scheduled for a specific month of the year—but conducted without notice. In Year 3 and beyond, walkthroughs might be conducted without notice at varying times of the year.

Once established, the walkthrough process might evolve in other ways as well. For example, walkthroughs might be conducted anonymously and without the presence of the clinic's clinic manager, nurse manager, or patient access services manager accompanying the compliance officer on his/her review. Such approaches are obviously more likely to present a more accurate picture of the clinic's typical operations and actual employee practices, because they do not allow the staff an opportunity to prepare the clinic for the visit. Walkthroughs could be conducted during different times of the day, including after office hours when staff have left the clinic and their workstations. The "no fault" spirit of the walkthroughs might be phased out as well as the program becomes institutionalized. Compliance reviews could cite individuals or clinics that put the privacy and security of patient information seriously at risk and violate institutional policy or applicable regulations. Completed checklists, results of the walkthrough, and recommendations from the compliance reviewers could be shared with a broader audience (i.e., middle management or leadership).

On one hand, these variations on the initial approach of the walkthroughs would increase their efficacy as a monitoring tool. In this respect, such changes would be beneficial and serve one goal of an effective compliance program. On the other hand, increased monitoring and the punitive character of the program would likely undermine the walkthrough's value as a collaborative exercise in which clinic staff and providers in the field work closely with the Privacy Office to develop effective procedures, processes, and practices to protect patient privacy. The more punitive the program, the less likely it will be to promote openness and cooperation. This unfortunate reality represents a delicate balance, the resolution of which should be made on an institution-by-institution basis. In the end, a Privacy compliance officer may have other effective ways to monitor employee behavior and, therefore, feel free to retain the walkthrough as an opportunity to meet staff as partners in a collaborative exercise to do the right thing and protect patient privacy.

1. DHHS, Office of Inspector General: "Elements of an Effective Compliance Program" in OIG Compliance Program for Individual and Small Group Physician Practices. 65 (194) F.R. 59434, October 5, 2000. Available at http://1.usa.gov/1np3hDY
2. Debbie Troklus and Greg Warner: *Compliance 101*, Third Edition (HCCA 2011), p. 66.