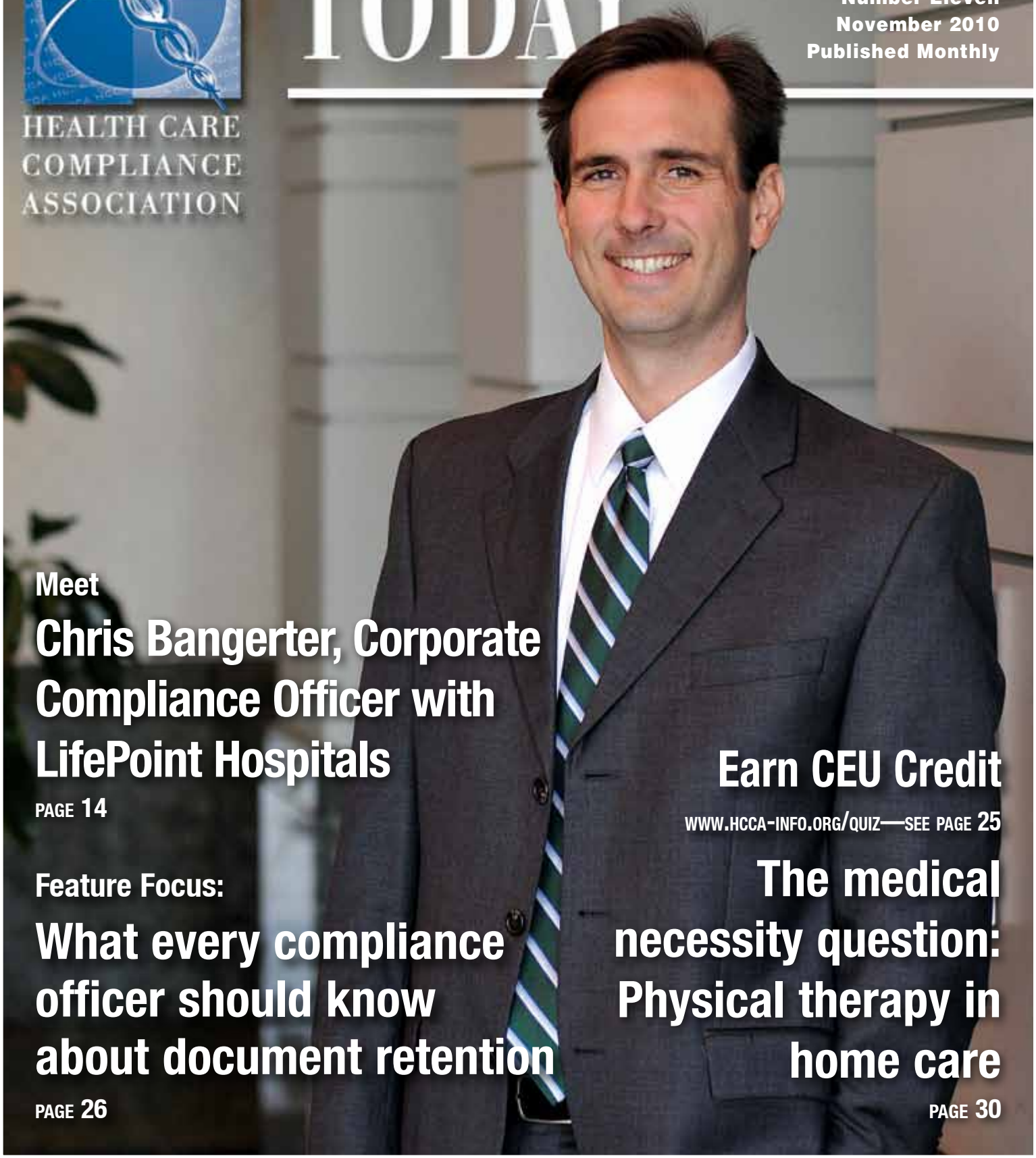
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Twelve
Number Eleven
November 2010
Published Monthly



Meet

Chris Bangerter, Corporate Compliance Officer with LifePoint Hospitals

PAGE 14

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ—SEE PAGE 25

Feature Focus:

What every compliance officer should know about document retention

PAGE 26

The medical necessity question: Physical therapy in home care

PAGE 30

feature focus

What every compliance officer should know about document retention

By Janice A. Anderson, Esq. and Tina Boschert, Esq.

Editor's note: Janice A. Anderson, Shareholder in the Chicago offices of Polsinelli Shughart PC, has over 25 years' experience focusing on health regulatory and compliance issues and over 30 years' experience working in the health care industry. She may be contacted by e-mail at janderson@polsinelli.com or by telephone at 312/873-3623.

Tina Boschert is an Associate in the Kansas City office of Polsinelli Shughart and may be contacted by telephone at 816/360-4118 or by e-mail at tboschert@polsinelli.com.

Tackling the issue of document retention in the normal course of business is often an insurmountable task for compliance officers, but it becomes even more challenging when your business is health care. Federal, state, and local rules often govern the documentation that needs to be retained and the retention period. Compliance officers need to be aware of how long documents must be retained and develop a comprehensive record retention program to address not only retention of records, but also their destruction. Documents must also be maintained appropriately to avoid charges that the organization has destroyed evidence. In addition, compliance officers must focus on the records created by the compliance program itself and establish appropriate time lines for retaining and destroying those records as well. This article will examine the general requirements and recommendations for an appropriate document retention/destruction policy for health care organizations and will specifically focus on how the policy should be applied to records created by the organization's compliance activities.

Document retention rules

Compliance officers are faced with a number of different rules and requirements regarding document retention. Several federal laws and regulations govern how long health care business documents should be retained. Most notable are those record retention requirements imposed by Health Information Portability & Accountability Act (HIPAA), The Department of Health and Human Services (DHHS), Occupational Health and Safety Act (OHSA), and the False Claims Act. Specifically, under the present HIPAA rules, a patient has up to six years to request an "accounting of disclosures" so "covered entities" should keep medical and other records of HIPAA compliance for at least six years. DHHS mandates that any records relating to Medicare contracts or reimbursements be retained for at least 5 years. OHSA requires that entities keep any employee exposure records, medical records, and analysis using such records for 30 years in addition to maintaining a log and records of occupation injuries and illnesses for 5 years. The Federal Civil False Claims Act (31 U.S.C. § 3729) allows either the government or private individuals to file actions against federal contractors, which include hospitals and other health care entities that participate in federal health care programs. Plaintiffs may allege fraud against the government, under some circumstances, for up to 10 years after the date on which the violation, or alleged violation, was committed. Therefore, a 10-year retention period is prudent for records, such as billing or compliance records.

In addition to federal laws and regulations, states may regulate the time frame that documentation should be retained. Compliance officers should review the applicable state retention requirements and check with state licensing authorities to determine whether any other document retention obligations exist under their state's laws. Accrediting agencies, such as The Joint Commission, also provide guidance regarding document retention, but do not typically mandate any specific record retention time frames. For example, The Joint Commission requires that hospitals retain records and information for sufficient periods of time to comply with the law and regulations and to support patient care, network management, legal documentation, research, and education. Lastly, when considering record retention, it is important to consider whether the entity has received notice of litigation. If notice has been given regarding possible litigation, relevant documents must then be retained indefinitely, until the litigation concludes, unless the court orders otherwise.

Establishing a comprehensive retention program

In light of the regulations surrounding record retention, it is critical that compliance officers develop and implement a comprehensive document retention program. The first step in the development of any such program should be to obtain a complete listing of all applicable retention requirements under both state and federal law. These retention requirements often have been collected by various trade associations and can be provided for a fee.

Next, all documents generated in the course of the organization's business need to categorized as to type of record (for example, financial records, patient records, legal records, etc). Health care organizations generate volumes of records on a daily basis. By grouping the records into categories, the applicable retention period can be identified as it applies to each category of record. For example, general business records may have different retention periods than patient health care records, other health care business records, tax records, etc. It is important to identify and categorize all records and, by reference to the specific retention requirements, identify how long each category of record must be maintained.

Similarly, it is important to identify all formats where documents may exist. Documents no longer exist in just paper format. E-mails and electronic media create and store records, and this information may be critical to retain as well. As electronic health records become more common, compliance officers should expect that electronic storage of records may become the rule rather than the exception. Compliance officers thus must determine all media where documents are created and stored in order to implement an appropriate document retention program.

Not only is it critical that compliance officers develop a policy regarding record retention that encompasses all required retention rules governing health care and business documentation, but the policy also must include a destruction schedule and procedure as well. The policy should clarify the category of records that need to be retained, the time frame for retention for each category, and should state an affirmative obligation to destroy the records at the conclusion of the retention period (along with the procedure and documentation to support such destruction). Destruction schedules and procedures should be developed, and care must be taken to ensure they are followed throughout the organization. Adhering to a destruction schedule and procedure helps establish that the destruction of the records occurred in the ordinary course of business. Without stating and adhering to a destruction schedule, an organization may find itself faced with charges that it intentionally destroyed documents for a nefarious purpose.

Key tips for establishing a record retention/destruction policy

- Identify all records that are created by the organization (coordinate with department directors and administration), categorize them according the type of record, identify which categories need to be retained, and determine the appropriate retention period.
- Create a comprehensive retention schedule that identifies by category the length of time the record should be maintained by the facility.
- Identify the record destruction date for each category of record.
- Draft a policy describing the record retention/destruction program and attach a schedule listing each category of record along with the retention period and the date for destruction.
- Include in the policy the procedure for destruction (how to destroy the records and the documentation that must be created to evidence the destruction).
- Educate and train staff regarding the document retention/destruction policy and their responsibilities in retaining and destroying records appropriately. Make sure it is followed.
- Secure proper storage of records, whether on-site or off-site, and maintain proper privacy and security of all stored (as well as active) records.

Likewise, the retention policy should identify who is responsible for maintenance and destruction for each type of record. This helps establish accountability for adhering to the record retention/destruction policy and makes it easier for the compliance officer to confirm that the policy is being followed. Documents evidencing destruction signed by the responsible person also should be retained according to a time frame that would ensure their availability if the destruction of a record is ever called into question. Creating a central repository for each type of document or record also may be helpful in monitoring compliance with the retention/destruction program.

Document retention policies must be in writing and should include the original policy along with any amendments or updated versions. Compliance officers should audit the document retention and destruction program to make sure it is being followed throughout the organization. These audit records also should be retained to evidence the facility's compliance program and demonstrate its efforts to comply with all record retention requirements.

Continued on page 28

 ...continued from page 27

Compliance program document retention strategies

Compliance program records, just as other records generated by the organization, need to be retained and destroyed appropriately. Compliance records should be separated into two general categories: compliance records that are generated in the ordinary course of business and compliance records that are generated under attorney-client privilege or in an investigation in anticipation of litigation.

Compliance records include general business records generated as a part of comprehensive compliance program. Examples of such records include screening audits of billing and coding activities, documentation of compliance education and training, evidence of compliance with OIG screenings for excluded providers, and investigations of complaints of compliance concerns received through the hotline or otherwise (unless conducted under attorney-client privilege), to name just a few. These records, as any other hospital business records, should be identified by the compliance officer, appropriately categorized by type of record, and retained/destroyed as a component of the comprehensive document retention/destruction program.

Compliance records generated under attorney-client privilege, or in anticipation of litigation, require precautions in addition to those provided to records generated in the ordinary course of the compliance program. In order to be protected under the attorney-client privilege or the work product doctrine, the document must be prepared for purposes of obtaining legal advice from an attorney to a client or prepared by an attorney for a client in anticipation of litigation. Although it is important to determine at the outset whether the compliance records should be created under privilege, it sometimes can be difficult to immediately ascertain whether a compliance matter will result in more serious enforcement action and therefore, should be investigated under the protection of the attorney-client/work product privileges. For this reason, compliance officers (even if they are also attorneys) are well advised to consult legal counsel early, if the nature of the issue may warrant attorney-client or attorney-work product protections. If a matter is to be conducted under the protection of the attorney-client or work product privileges, it is crucial to establish the privilege in writing, identify specifically who is part of the work team to investigate the issue, and then appropriately identify and segregate the privileged documents for retention purposes.

Any documents regarding an investigation that is conducted under privilege and prepared by outside counsel, by the hospital attorney, by the compliance officer (who may be the hospital attorney), or by someone else at the direction of an attorney should be appropriately identified as privileged, and limited in distribution. All documents created under the privilege should be prominently identified as "subject to the attorney-client or attorney-work product privileges." These documents should be disseminated only to those individuals who have been identified in writing as part of the work team and who need to either participate in the investigation or know the information for legitimate purposes.

This is equally true if the communication is by e-mail. Whether the document is attached in an e-mail or the document is the "body" of the e-mail itself, its distribution should be limited in scope and the document and/or the e-mail should be prominently labeled as "work product" and/or "privileged and confidential." Care also must be taken to prevent e-mail distribution other than to those recipients who need to know the information for purposes related to this investigation. E-mail communication of confidential and privileged information presents significant issues in maintaining the privileged nature of the information, because forwarding such communication/documentation is often easy to do (even inadvertently), potentially waiving the privilege. Thus, it may be prudent for the compliance officer to evaluate the extent to which e-mail should be used for communication when an investigation is occurring at the direction of an attorney and whether electronic retention of privileged materials should occur. It may be safer to print e-mails generated in a compliance investigation and retain them only in hard copy in the compliance investigation/legal file. Keep in mind that, if this option is chosen, extra steps must be taken to delete the privileged items from computer hardware and servers as well.

Even when an investigation is properly conducted under attorney-client/work product privileges, not all documents related to the matter will be privileged, and it is necessary to distinguish what is protected from what is discoverable. Medical records, policies, routine audits, accounting statements, and contracts are all examples of documents that would be discoverable, even if collected under an otherwise privileged investigation. Likewise, any documents, audits, memos, etc. prepared prior to seeking legal advice or not in "anticipation of litigation" are also going to be discoverable, even if they are subsequently given to an attorney. For example, if the medical records director prepares a memo to the compliance officer describing concerns relating a substantial overpayment and/or the possibility of Medicare fraud, this document likely will not be protected, even if it later is given to an attorney. Accordingly, it is important for the compliance officer to establish a procedure for reporting more serious compliance issues that involves taking advantage of the attorney-client protections and for

distinguishing those records that are subject to the privilege from those that are not.

An important reason to separate the privileged communications and/or documents from other discoverable documents relates to the storage of the records. Privileged records should be stored in a separate, secure location and prominently identified as privileged. This allows for immediate identification of privileged records in the event the organization is confronted with a government agency seeking production of documents through a search warrant. It is far easier to attempt to avoid turning over privileged information in the first instance than to try to get it back once it has been confiscated. Further, if numerous privileged documents/and or communications exist related to a single compliance issue, it may be prudent to create a privilege log to quickly distinguish the privileged information from the other non-privileged information contained in the file.

Conclusion

Development of a comprehensive record retention program is no easy task. It is important to be aware of federal and state rules that govern what records need to be retained and the applicable retention time frames. It is equally important to develop a comprehensive record retention program to implement these retention requirements. That program should address not only retention, but also destruction of records. Compliance officers also must pay particular attention to the records created in the compliance program itself. They must segregate general compliance records from those records that are protected under the attorney-client and work product privileges, identify and store the records carefully, and establish appropriate time lines for retaining and destroying these records as well. Taking such steps will help ensure that the organization complies with the law, has the records it needs for its own purposes, and can appropriately defend itself from claims that can arise when business records are not appropriately retained and destroyed. ■