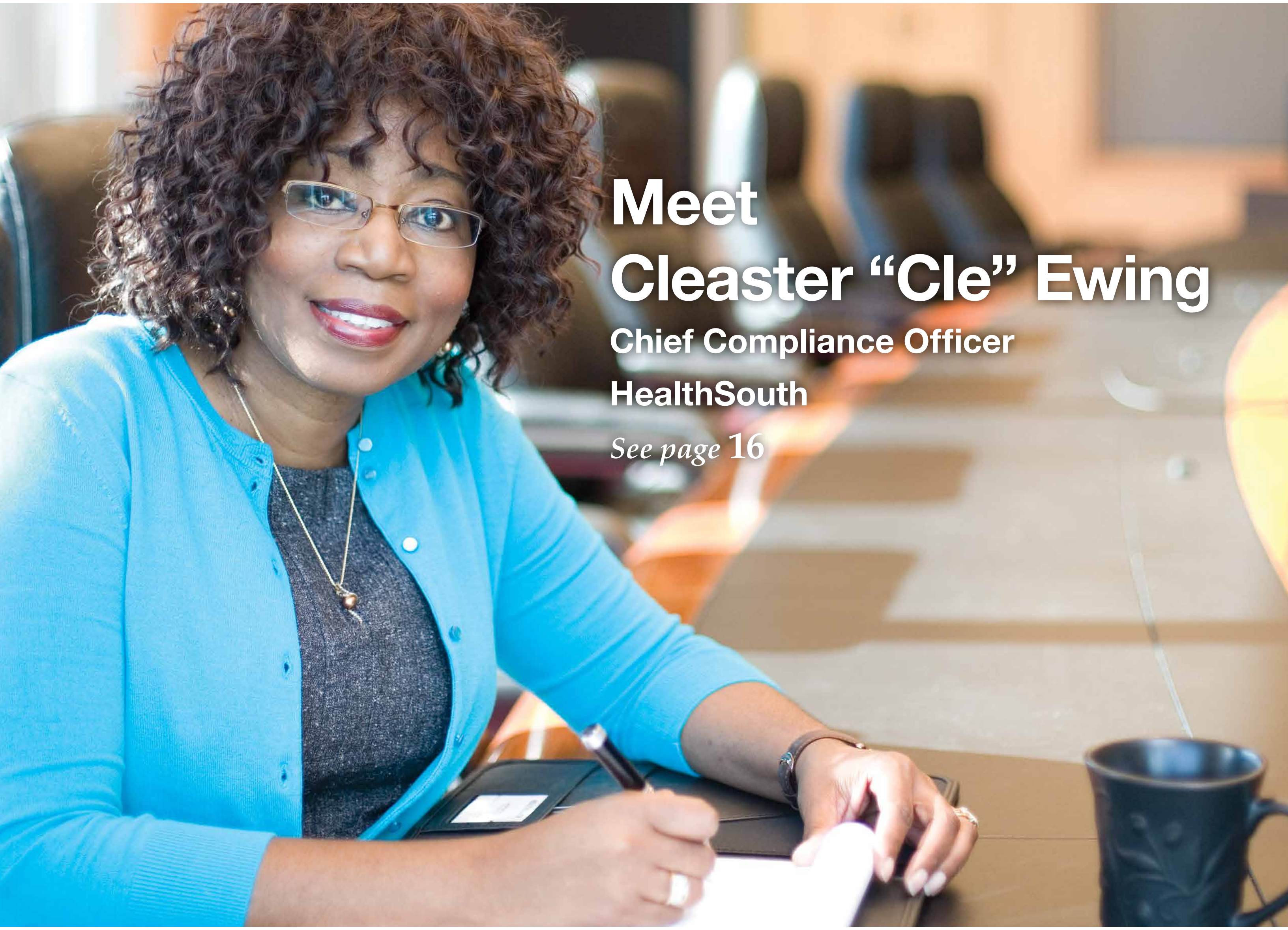
HCCA
HEALTH CARE
COMPLIANCE
ASSOCIATION

Compliance TODAY

December 2012

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Meet Cleaster "Cle" Ewing

Chief Compliance Officer

HealthSouth

See page 16

by Kimberly J. Gold

Utilizing the HIPAA audit protocols as a compliance tool

» Covered entities are now subject to privacy and security audits by OCR.

» OCR published audit protocols regarding its standards for such audits.

» The audit protocols cover the HIPAA Privacy Rule, Security Rule, and Breach Notification requirements.

» Policies and procedures and documentation are of utmost importance to auditors.

» The audit protocols should be used as a compliance tool.

***Kimberly J. Gold** (kjgold@mintz.com) is an attorney in the New York City offices of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC.*

Gold

In order to ensure that covered entities comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] Privacy and Security Rules and Breach Notification requirements,[2] and as mandated by the Health Information Technology for Economic and Clinical Health Act (HITECH), the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) has begun performing privacy and security audits of covered entities. OCR initiated a pilot audit program to perform 115 audits of covered entities between November 2011 and December 2012,[3] and this pilot program has helped OCR refine the HIPAA requirements that it will assess during its audits. In June 2012, OCR published audit protocols that provide more clarity on auditors' standards for performing HIPAA compliance audits of covered entities and business associates.[4]

Key areas of focus

The audit protocols cover the three primary areas of HIPAA privacy and security enforcement:

1. Privacy Rule requirements, including:

- Notice of Privacy Practices for protected health information (PHI)
- Rights to request privacy protection for PHI
- Access of individuals to PHI
- Administrative requirements
- Uses and disclosures of PHI
- Amendment of PHI
- Accounting of disclosures.

2. Security Rule requirements for administrative, physical, and technical safeguards.

3. Breach Notification requirements.

The protocols establish 165 performance criteria, 77 of which focus exclusively on compliance with the Security Rule, and 88 of which collectively address the Breach Notification and Privacy Rule requirements. The protocols essentially mirror the requirements of the HIPAA Privacy, Security, and Breach Notification rules, but provide greater insight into what covered entities and business associates can expect if selected for an audit.

Audit protocol contents

The audit protocols differ based on the particular performance criteria being assessed, but there are recurrent themes that demonstrate what auditors will be looking for. For example, most of the protocols direct auditors to inquire of management as to whether formal or informal policies or procedures exist for a given performance standard, and whether such policies and procedures have been approved and updated on a periodic basis. The protocols also generally direct auditors to obtain and review policies and procedures and other evidence and/or documentation relevant to the specified criteria. The protocols frequently require auditors to confirm that HIPAA policies and procedures and updates to those policies and procedures are properly communicated to the workforce.

> It is important to note that, like the corresponding rules themselves, the Security Rule audit protocols are divided into "required" and "addressable" categories. If an organization has chosen not to implement a given "addressable" requirement, it must provide documentation supporting its decision.

It is important to note that, like the corresponding rules themselves, the Security Rule audit protocols are divided into "required" and "addressable" categories. If an organization has chosen not to implement a given "addressable" requirement, it must provide documentation supporting its decision.

Applying the protocols to compliance efforts

OCR has indicated that it will continue to conduct audits of covered entities through 2013 and 2014, and such audits will be expanded to cover business associates after the publication of the HIPAA Omnibus Rule.[5] The audits are intended to serve as a "compliance improvement tool" used to measure compliance with the HIPAA requirements. Such audits may uncover compliance issues that the subject entity can address through corrective action, though the audits may reveal serious compliance problems that could lead to a separate OCR enforcement investigation.[6] Accordingly, it is essential for covered entities and business associates to review and understand the audit protocols and to evaluate and tailor their HIPAA policies and procedures accordingly.

Organizations should perform periodic self-assessments of their HIPAA policies and procedures and should use the audit protocols as a checklist against their current compliance efforts. Any items that would not meet the OCR's audit requirements should be revised proactively so that they do not become areas of non-compliance. Organizations should also ensure that all employees are trained on the privacy, security, and breach notification requirements that OCR is focused on in connection with its audits.

Because the protocols require robust documentation of written policies and procedures, organizations must have extensive documentation detailing their HIPAA policies and procedures. Such documentation should be comprehensive, organized, and easy for OCR auditors to review and understand. For any addressable Security Rule requirements that an entity has decided not to implement, there must be documentation supporting the decision.

According to Linda Sanches, OCR Senior Advisor, Health Information Privacy Lead, HIPAA Compliance Audits, covered entities should also prepare for audits by identifying the location of all PHI and tracking PHI movement within the organization and as exchanged with third parties.[7] Because OCR has indicated that "every covered entity and business associate is eligible for an audit,"[8] in addition to being prepared for their own audits, covered entities should also convey their expectations to business associates so that business associates can be mindful of the audit protocols and their compliance obligations.

Conclusion

The HIPAA audit protocols can serve as a useful guide for compliance with HIPAA requirements and preparing for potential audits. In reviewing and updating their compliance programs, covered entities and business associates should remember the following key items of importance to auditors:

- Policies and procedures for privacy, security, and breach notification requirements;
- Evidence of periodic updates to policies and procedures;
- Workforce training on HIPAA compliance, including policy and procedure updates;
- Explanation for unaddressed Security Rule requirements; and
- Extensive documentation.

[1] 42 U.S.C. §§ 300gg et seq., P.L. 104-191.
[2] Health Information Technology for Economic and Clinical Health (HITECH) Act § 13411.
[3] Office of Civil Rights, Health Information Privacy: "Audit Pilot Program." Available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html.
[4] Office of Civil Rights, Health Information Privacy: "Audit Protocol." Available at http://ocrnotifications.hhs.gov/hipaa.html.
[5] David Mayer, Senior Advisor, Office of Civil Rights, Presentation at the 2012 American Health Lawyers Association Annual Meeting: OCR HIPAA Audits and Responding to Breaches (June 25, 2012).
[6] Linda Sanches: "2012 HIPAA Privacy and Security Audits," United States Department of Health & Human Services, Office of the Secretary, Office for Civil Rights. Available at http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.
[7] *Id.*
[8] "Audit Pilot Program," *supra* note 3.