HHS Issues New HIPAA Privacy, Security, and Breach Notification Audit Protocol

In April 2016, the Department of Health and Human Services’ Office for Civil Rights (“OCR”) released its updated HIPAA Privacy, Security, and Breach Notification Audit Protocol in anticipation of launching its Phase 2 Audit Program. In mid-July, OCR officially began its Phase 2 Audits by emailing notices to 167 covered entities (which include health plans, healthcare providers, and healthcare clearinghouses). OCR’s intent behind its new audit program is to review the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. Business Associates were not included in the mid-July audits, but will be included in the next round of audits occurring later this year.

Employers sponsoring health plans should take steps to familiarize themselves with the audit program and the audit protocol.

The Audit Program

Background

The Health Insurance Portability and Accountability Act (“HIPAA”) established national standards for the Privacy and Security of protected health information (“PHI”). The Privacy Rule standards address the use and disclosure of PHI by organizations subject to the Privacy Rule – called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting PHI that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that covered entities must put in place to secure individuals’ “electronic protected health information” (“ePHI”).

The Health Information Technology for Economic and Clinical Health Act (“HITECH”) amended HIPAA to establish Breach Notification requirements. Under the Breach Notification requirements, a covered entity must notify the Secretary of Health and Human Services if it discovers a breach of unsecured PHI. PHI is unsecured if it is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through specific processes acceptable under HIPAA, such as shredding for paper PHI and encryption for ePHI.

HITECH requires the OCR to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by 115 covered
entities to comply with HIPAA’s requirements. Based upon the pilot audit program (also called the Phase 1 audit program), OCR prepared to implement Phase 2 of its audit program, which will audit both covered entities and business associates. As part of this program, OCR developed enhanced protocols (sets of instructions) to be used in Phase 2 audits and will also test the effectiveness of desk audits in evaluating the compliance efforts of the HIPAA regulated industry. A desk audit does not involve an on-site audit, which means that an OCR representative will generally be restricted to reviewing documents provided by an auditee.

*Eligibility for an Audit*

OCR may select any covered entity or business associate for an audit. Such entities include covered individual and organizational providers of health services, such as physicians or hospitals; health plans of all sizes and functions, such as Medicaid organizations or employer-sponsored health plans; healthcare clearinghouses, such as health care provider billing services; and a range of business associates of those entities. Employer-sponsored health plans include medical, dental, vision, health flexible spending account (“FSA”), health reimbursement arrangement (“HRA”), most employee assistance programs (“EAPs”), and some long-term care benefits.

*Selection for Audit*

OCR identifies pools of covered entities and business associates that represent a wide range of healthcare providers, health plans, healthcare clearinghouses, and business associates. The entities selected are intended to represent different categories of size, type, and operations. Sampling criteria for selection include size of the entity, affiliation with other healthcare organizations, the type of entity and its relationship to individuals, whether an organization is public or private, geographic factors, and present enforcement activity with OCR. OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review.

OCR will first contact entities to obtain data about size, type, and operations. That initial data is used to create pools of potential auditees. OCR then randomly selects auditees from the pools. Entities selected for an audit will be sent an email notification of their selection and will be asked to provide documents and other data in response to a document request letter. Auditees will have only ten business days to respond. Audited entities will submit documents on-line via a new secure audit portal on OCR’s website. Although OCR intends to conduct fewer on-site visits during Phase 2 audits than during the Phase 1 audits, auditees should be prepared for a site visit if OCR deems it appropriate. Generally, however, the audits will be focused upon specific compliance areas. For example, the first round of Phase 2 desk audits focuses on the following compliance areas:

<table>
<thead>
<tr>
<th>Requirements Selected for Desk Audit Review</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Rule</strong></td>
</tr>
<tr>
<td>Notice of Privacy Practices &amp; Content Requirements</td>
</tr>
<tr>
<td>Provision of Notice – Electronic Notice</td>
</tr>
<tr>
<td>Right to Access</td>
</tr>
<tr>
<td><strong>Breach Notification Rule</strong></td>
</tr>
<tr>
<td>Timeliness of Notification</td>
</tr>
<tr>
<td>Content of Notification</td>
</tr>
<tr>
<td><strong>Security Rule</strong></td>
</tr>
<tr>
<td>Security Management Process – Risk Analysis</td>
</tr>
</tbody>
</table>

Auditors will review documentation and then develop and share draft findings with the entity. Auditees will have the opportunity to respond to these draft findings; their written responses will be included in the
final audit report. Audit reports generally describe how the audit was conducted, discuss any findings, and contain entity responses to the draft findings.

**The Audit Protocol**

The audit protocol is a lengthy, detailed protocol. It is available via this [LINK](#). OCR intends to release a downloadable version in the future, but the current protocol may at least be accessed online.

The protocol is broken down by audit type (Privacy, Security, or Breach Notification), reference section to the regulations, key activity (e.g., disclosures to personal representatives), established performance criteria (i.e., the standard against which compliance will be measured), and audit inquiry (i.e., what the auditor will seek). For Security measures, the protocol also includes an indication as to whether the standard is required or addressable. Required Security measures are mandatory, and all covered entities must comply. Addressable Security measures are not required, but if a covered entity does not adopt an addressable safeguard, it must adopt and document an alternative.

Because the audit protocol was updated to incorporate Omnibus HIPAA regulations released in 2013, there are a few new items employers should note. First, the audit protocol now seeks information about compliance with HIPAA restrictions on the use of genetic information for underwriting purposes. If audited, employers with wellness programs may be asked to provide any questionnaires or health risk assessments provided in conjunction with their benefits. Second, the audit protocol includes more specific questions addressing details in the Notice of Privacy Practices such as contact information (including a name or title and a phone number) for further information (i.e., for the HIPAA Privacy Officer) and an effective date of the Notice of Privacy Practices.

In addition, the audit protocol now includes more specific questions to direct an auditor’s review. For example, under the audit inquiry for compliance with the Evaluation standard under the Security Rule, auditors will not only seek documentation of policies and procedures related to a technical and nontechnical evaluation of security measures, but will also review those policies and procedures to determine if the covered entity has identified:

- The means by which findings, remediation options, and recommendations are evaluated;
- Whether the policy and procedures require that the evaluation will be repeated on a periodic basis and/or when environmental or operational changes are made or newly recognized risks affect the security of ePHI; and
- Whether the policies and procedures state the frequency of when to conduct the next evaluation to update the current policy and procedures.

Thus, current policies and procedures should be reviewed to determine whether they address the information sought under the audit inquiry standards.

If audited, a covered entity will be required to provide documents which may include policies and procedures or documents demonstrating compliance with a specific standard. For example, a covered entity may be asked to provide its policy for disclosures to public officials and documentation demonstrating that the covered entity verified the identity of appropriate public official such as by obtaining a letter from the official on official agency letterhead (if applicable). When responding to an
audit, entities must provide only the specified documents, not collections of all the entity’s policies or procedures. The auditor will not search for relevant documentation that may be contained within compilations. Thus, it would be wise for an auditee to clearly label or otherwise signal which documents are responsive to each audit standard. Further, unless otherwise specified, all document requests are for versions in use as of the date of the audit notification and document request. Thus, it is important to have easy access to all current policies and procedures.

Resources

OCR webpage with the audit protocol: [http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html](http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html)


OCR HIPAA webpage for Professionals: [http://www.hhs.gov/hipaa/for-professionals/index.html](http://www.hhs.gov/hipaa/for-professionals/index.html)


Employer Action Steps

Employers should review all existing HIPAA policies and procedures with an eye toward determining whether those policies and procedures meet the standards established by the new HIPAA audit protocol. Employers that do not have current policies and procedures should work to establish written policies and procedures as soon as possible. Further, employers should evaluate steps taken to document compliance such as documentation of certain disclosures of PHI, verification of the identity of those seeking access to PHI, responding to requests for individuals’ rights (such as the right to inspect and copy), breach notification timeliness (if applicable), and content of any breach notification (if applicable).

Compliance with the HIPAA Privacy, Security, and Breach Notification Rules is necessary not only to pass an audit by OCR, but also to help protect an employer against mishandling of PHI by workforce members carrying out activities on behalf of the employer’s health plans. As recent Compliance Resolution Agreements have shown, failure to comply with the Rules, even without a breach of unsecured PHI, can lead to monetary payments of hundreds of thousands of dollars to millions of dollars. Thus, employers should take action to ensure compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

Gallagher Benefit Services, through its compliance experts and consultants, will continue to monitor developments on HIPAA legislation and regulation and will provide you with relevant updated information as it becomes available. In the interim, please contact your Gallagher Benefit Services Representative with any questions that you may have.

---

*The intent of this Technical Bulletin is to provide general information on employee benefit issues. It should not be construed as legal advice and, as with any interpretation of law; plans sponsors should seek proper legal advice for the application of these rules to their plans.*