Office for Civil Rights
HIPAA Privacy, Security, & Breach Notification Audit Program

Draft Report

<Hospital> 03/21/2017

*Entities must **provide any responses within 10 business days** of receipt of this document in order for OCR to include them in the final audit report. Entities may provide responses via email to OSOCRAudit@hhs.gov:*

1. *in the body of an email, or*
2. *using a MS Word attachment.*

Please identify each response with the corresponding element number and name, as presented in this report, auditor analysis and findings section. Do not submit new documentation, as it will not be considered.

Introduction

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS), has conducted a desk audit of <Hospital>. This audit examined entity compliance with key aspects of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy, Security and Breach Notification Rules. This document is the draft report of findings. It may serve as a resource for ongoing entity compliance activities. Any findings reveal opportunities for the entity to improve its protection of protected health information and its provision of individual rights. Further guidance may be found at http://www.hhs.gov/hipaa/for-professionals/index.html.

<Hospital> is a Provider located in City, State.

Audit Objective

The audit program is an important part of OCR's overall health information privacy, security, and breach notification compliance activities. OCR uses the audit program to assess the compliance efforts of a range of entities covered by the HIPAA Rules. The audit program offers covered entities and business associates insight into OCR expectations for compliance and tools for self-assessment. The audits present OCR an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through ongoing complaint investigations and compliance reviews, and get out in front of problems before they result in breaches. OCR will share any best practices gleaned through the audit process and plans to issue guidance targeted to identified compliance challenges.

Background

HIPAA mandates the protection of PHI from impermissible use and disclosure. The HHS Office for Civil Rights has responsibility for administering and enforcing the HIPAA Privacy, Security and Breach Notification Rules (altogether, the Rules). The Rules provide important health information privacy and security protections and specify the rights of individuals regarding their PHI.

The American Recovery and Reinvestment Act of 2009 (ARRA), in Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), requires HHS to perform periodic audits of covered entity and business associate compliance with the Rules. Covered entities (CE) include health plans, health care clearinghouses and health care providers who electronically conduct certain administrative and payment-related transactions. A business associate (BA) is a person or entity that creates, receives, maintains or transmits PHI as it performs certain functions or activities on behalf of, or provides certain services to, a covered entity or another business associate.

Over 2016 and 2017, OCR is conducting two types of desk audits of covered entities. The desk audits of covered entities examine compliance efforts related to either: 1) the risk analysis and risk management provisions of the Security Rule; or 2) the access and notice provisions of the Privacy Rule and the applicable content and timeliness provisions of the Breach Notification Rule. The business associate desk audits focus on the risk analysis and risk management provisions of the Security Rule, and the applicable content and timeliness provisions of the Breach Notification Rule. See the *Selected Protocol*

Elements Guidance for more information about the audited elements; http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf. In 2017, OCR is also conducting on-site audits of both covered entities and business associates. The on-site audits are broader than the desk audits in that they review compliance activities related to a comprehensive set of requirements of all three rules and involve additional analysis.

Scope and Methodology

In carrying out the desk audits, OCR assesses the submitted policies, procedures and other requested documentation against the inquiries specified in the audit protocol. The audit protocol used for this assessment is available on the OCR audit webpage; http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit.

<Hospital> was informed by OCR of its selection for audit and was asked to provide certain documentation related to its compliance efforts. OCR reviewed the information provided to identify and analyze the processes, controls, or policies against the criteria in the audit protocol.

OCR is submitting draft findings to <Hospital> to provide it with the opportunity to respond with comments or descriptions of any completed or planned corrective actions. The OCR auditors will consider <Hospital>'s responses in finalizing the analysis. The final report will incorporate comments and description of any corrective actions that were submitted by <Hospital> and OCR's assessment of those comments, as appropriate.

Results of Review

Any preliminary findings of indications of noncompliance are listed below. In addition, OCR assessed a relative level of entity compliance efforts for each audited element on a scale of 1 through 5. The scores indicate OCR's assessment of the comprehensiveness and effectiveness of these efforts and the magnitude of related risk: See *Compliance Effort Ratings – Legend*, below, for more information. While audited entities should remediate all findings, higher scores indicate that OCR believes that timely and complete corrective action by the entity is essential.

Auditor Ratings

The auditor assessed entity efforts to comply with the selected elements using the following guidelines.

Compliance Effort Ratings—Legend	
Rating	**Description**
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.

Summary of Auditor Ratings

Rule	Element #, Section and Key Activity	Draft Rating
Breach	BNR12 §164.404(b) Timeliness of Notification	1
Breach	BNR13 §164.404(c)(1) Content of Notification	4
Privacy	P65 §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3) Right to access	4
Privacy	P55 §164.520(a)(1) & (b)(1) Notice of Privacy Practices Content requirements	3
Privacy	P58 §164.520(c)(3) Provision of Notice - Electronic Notice	1

Auditor Analysis & Findings

This section describes the auditor's analysis and findings. Any findings reveal opportunities for the entity to improve its protection of PHI and implementation of individual rights. Entities can find guidance for their efforts on http://www.hhs.gov/hipaa/for-professionals/index.html.

Element #	SECTION	KEY ACTIVITIES
BNR12	§164.404(b)	Timeliness of Notification
Preliminary Finding	1) None.	
Preliminary Auditor Analysis	The entity provided a summary of breach incidents, and individuals were notified within 4, 18, 21, 17, and 12 days, respectively, of breach.	
Preliminary Rating	1	
Effect	Failure to provide a breach notification without reasonable delay or within 60 days of breach discovery may adversely impact the rights of the individuals who are subject to the breach	

Element #	SECTION	KEY ACTIVITIES
P65	§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)	Right to access
Preliminary Finding	1) The entity did not provide adequate evidence that it has policies and procedures in place that permit an individual to request access to inspect or to obtain a copy of PHI about the individual that is maintained in a designated record set consistent with the access standard and implementation specifications. 2) The entity did not provide adequate evidence that it provides the access requested consistent with the requirements of the access standard and implementation specifications.	
Preliminary Auditor Analysis	The entity does not have a standard access request form, but the entity does require requests to be made in writing. The entity's Notice of Privacy Practices does not state the patient's right to timely access, which is generally within 30 days of the request. The entity does not charge a reasonable, cost based fee for providing summaries of records. The entity's policy does not include all requirements related to processing record requests. The policy does not address requests for records not maintained by the entity. The entity provided documentation of access requests and verification, but it did not provide evidence of the documents provided to the requestors, making it impossible to evaluate the extent of compliance with the individual's request or consistency with this standard.	
Preliminary Rating	4	
Effect	Failure to allow and facilitate an individual’s access to his/her PHI may limit the individual’s lawful rights to access and receive a copy of important health information contained in their medical records or within a designated record set.	

Element #	SECTION	KEY ACTIVITIES
P55	§164.520(a)(1) & (b)(1)	Notice of Privacy Practices Content requirements
Preliminary Finding	1) The notice does not include all required elements.	
Preliminary Auditor Analysis	The notice fails to include several requirements, specifically: • The notice does not include a statement that the CE is required to disclose PHI to the Secretary of HHS. • The notice does not include a statement that the entity is required to disclose upon request, to the individual or other person named by the individual, an electronic or paper copy of PHI. • The notice does not include a statement that the use or disclosure of psychotherapy notes requires individual authorization. • The Notice of Privacy Practices does not contain a description of how the individual may exercise the right to obtain a copy of the individual's health and claims records, and to direct the covered entity to send these records to a third party.	
Preliminary Rating	3	
Effect	Failure to adequately and comprehensively provide individuals with a notice of privacy practices for protected health information could result in an individual not knowing how his/her protected health information is used or disclosed; not knowing what individual rights they have with respect to their protected health information; and/or not knowing the extent of the entity's legal duties with respect to the protected health information.	

Element #	SECTION	KEY ACTIVITIES
P58	§164.520(c)(3)	Provision of Notice - Electronic Notice
Preliminary Finding	1) None.	
Preliminary Auditor Analysis	The entity maintains its Notice of Privacy Practices via a link under the "About Us" drop down menu on the top of the home webpage and link at the bottom of the home page. The entity does not provide its Notice to patients via email or other electronic means, so this aspect of the control is not applicable.	
Preliminary Rating	1	
Effect	Failure to provide electronic notice of privacy practices may result in an individual not being informed of his/her rights, or the entity's duties, regarding the use and disclosure of the individual's protected health information.	