Provided by BB&T Insurance Services, Inc., McGriff, Seibels & Williams, Inc., BB&T Insurance Services of California, Inc., and Precept Insurance Solutions, LLC

HIPAA Compliance Reviews – Audit Protocol

Legislative Alert 6-2016 April 18, 2016

HIPAA Audit Program:	▪ The second phase of the HIPAA audit program is underway. ▪ Covered entities and business associates may be selected for a HIPAA audit. ▪ OCR published a protocol that describes its standards for HIPAA audits.
HIPAA Self-Audits:	▪ To prepare for a possible audit, health plan sponsors and business associates should self-audit their compliance with the HIPAA rules. ▪ OCR's audit protocol can be used as a guide for self-audits of HIPAA compliance. ▪ The SRA Tool can also be used to perform and document an entity's security risk analysis.

The Department of Health and Human Services (HHS) has launched the second phase of its HIPAA audit program, which focuses on compliance with HIPAA's Privacy, Security and Breach Notification Rules. HHS' Office for Civil Rights (OCR) is responsible for conducting these audits.

This second phase of the HIPAA audit program covers both covered entities and business associates. According to OCR, these HIPAA audits are primarily a compliance improvement activity. However, if an audit reveals a serious compliance issue, OCR may initiate a compliance review to investigate.

In connection with this second phase of HIPAA audits, OCR released an **updated audit protocol** that identifies potential areas of audit inquiry. To prepare for a possible HIPAA audit, covered entities and business associates should review their compliance with HIPAA's Rules and make any necessary changes. OCR's audit protocol can be used as a guide for self-audits of HIPAA compliance.

Links and Resources

- OCR's audit protocol for covered entities and business associates
- HIPAA's Security Risk Assessment Tool (SRA Tool)
  - Download the SRA tool here
  - SRA Tool User Guide
  - SRA User Videos

Also, even if a health plan or business associate is not selected for a Phase 2 audit, it is still important to remain prepared for a HIPAA compliance review – OCR will likely continue its enforcement efforts after the Phase 2 audits are complete.

Audit Protocol

OCR published an **audit protocol** to provide clarity on the HIPAA standards that auditors may assess during an audit. OCR first made its HIPAA audit protocol available in 2012 in connection with its pilot audit program. In 2016, OCR released an updated audit protocol, which includes changes made by the HIPAA Omnibus final rule from 2013.

The audit protocol is organized around modules, representing separate elements of privacy, security and breach notification. The updated audit protocol identifies approximately 180 areas for potential audit inquiry. According to OCR, the areas that are assessed during an audit will vary based on the type of covered entity or business associate selected for review.

OCR's audit protocol can be used as a guide for self-audits of HIPAA compliance.

The audit protocol identifies "key activities" (HIPAA standards) and provides information on the legal requirements for each standard ("established performance criteria"), as well as potential audit inquiries related to the HIPAA requirements.

Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	Required/ Addressable
Privacy	§ 164.502 (a)(5)(i)	Prohibited uses and disclosures – Use and disclosure of genetic information for underwriting purposes	§ 164.502 (a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of	Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history? Inquire of management.	

Also, although the audit protocol's requirements depend on the specific HIPAA standard being assessed, there are some recurring themes that indicate what the auditors may be looking for. For example, many of the protocols direct auditors to ask whether policies or procedures exist for a given HIPAA standard, and whether these policies and procedures have been updated on a periodic basis.

HIPAA Self-Audits

Covered entities and business associates should perform periodic self-assessments of their HIPAA compliance and can use the audit protocol as a guide during this process. If a covered entity or business associate discovers an area of noncompliance, it should take steps to remedy the problem.

Based on the audit protocol's recurring themes, a HIPAA self-audit should emphasize the following HIPAA standards:

- Does the covered entity or business associate have the required HIPAA policies and procedures for privacy, security and breach notification in place?
- Have there been periodic updates to these policies and procedures?
- Has the covered entity or business associate trained its workforce on HIPAA compliance, including any policy and procedure updates?
- Has the entity performed a risk analysis to assess the potential risk and vulnerabilities for its electronic PHI (ePHI)?
- If an entity has decided not to implement an "addressable" security standard, does it have documentation supporting its decision?

Also, to prepare for a potential audit, an organization should confirm that its HIPAA documents (including its policies and procedures) are comprehensive, well-organized and easy to comprehend.

Privacy Rule Requirements

The audit protocol includes 89 areas of potential audit inquiry under the HIPAA Privacy Rule. For example, the audit protocol includes compliance questions regarding the Privacy Rule's:

- Use and disclosure rules
- Minimum necessary standard
- Privacy notice requirement
- Business associate contract requirement
- Individual rights requirements

Special rules for fully insured health plans

How the HIPAA Privacy Rule impacts the sponsor of a fully insured plan depends on whether the plan sponsor has access to PHI for plan administration purposes. Sponsors of fully insured plans that do not have access to PHI are only subject to a few of the Privacy Rule's requirements. Sponsors of fully insured plans that have access to PHI and sponsors of self-funded plans, however, have additional compliance obligations under the Privacy Rule.

Security Rule Requirements

The audit protocol includes 72 potential areas of audit inquiry that address the HIPAA Security Rule's requirements for administrative, technical and physical safeguards for ePHI. Under the Security Rule, each type of safeguard has certain standards and implementation specifications associated with it. In an effort to provide covered entities and business associates with some flexibility, the Security Rule provides two categories of implementation specifications – "required" and "addressable." While addressable implementation specifications are not optional, organizations have more options in determining how they will comply with these requirements.

Compliance Tip

If a covered entity or business associate decides not to implement an addressable specification (or if it implements an alternative standard), the entity must **document the reasons** for its decisions, including why it determined that the addressable specification was not a reasonable and appropriate safeguard.

The audit protocol also addresses whether the entity has performed a **risk analysis** to assess the potential risks and vulnerabilities to all of the ePHI that it creates, receives, maintains or transmits. Conducting a risk analysis is a **crucial first step** in an organization's efforts to comply with the Security Rule. The risk analysis directs what reasonable steps a covered entity or business associate should take to protect the ePHI it creates, transmits, receives or maintains. Failing to conduct a timely and thorough risk assessment has routinely been identified by OCR as a common HIPAA compliance problem.

HHS, through its Office of the National Coordinator for Health Information Technology (ONC), has developed an interactive Security Risk Assessment Tool (SRA Tool) to assist organizations in performing and documenting security risk assessments.

The SRA Tool is a software application that can be used by a covered entity or business associate as a resource (among other tools and processes) to review its implementation of the HIPAA Security Rule. HHS has also provided a User Guide and tutorial video to help organizations begin using the SRA Tool.

Breach Notification Rules

The audit protocol addresses HIPAA's breach notification requirements for unsecured PHI, and, in addition to other breach notification standards, instructs auditors to review covered entities' policies and procedures regarding breach notification. For example, the protocol asks whether the covered entity has policies and procedures in place for determining whether an impermissible use or disclosure triggers a breach notification requirement.

The HIPAA Omnibus final rule from 2013 changed some of the standards for determining whether a breach notification is required. As part of their HIPAA compliance review, covered entities should make sure that their breach notification policies have been updated for the final rule and that their workforce has been trained on the notification standards.