BURR ALERT

Phase 2 HIPAA Audits

The Burr & Forman Health Care Group June 2016

In an effort to review and examine compliance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"), the Department of Health and Human Services Office for Civil Rights ("OCR") is conducting Phase 2 HIPAA audits for both covered entities and business associates. OCR is conducting the audits to assess new risks, identify effective privacy and security measures, and develop targeted guidance on specific areas of concern.

The first step in the audit phase is a pre-audit screening email sent to potential auditees. We have seen several of these delivered recently. A sample of the pre-audit screening email can be found here. The email contains a questionnaire addressing size, entity type, services, contact information, and other background information. The online questionnaire must be completed and returned to OCR within 30 days. Based on the responses received and the information gathered, OCR will create a smaller, representative sample audit pool. Thus, not all entities that receive the initial pre-audit screening email will be audited. However, failure to respond to the questionnaire will not remove an entity from the audit selection pool. OCR will use publicly available information about an entity if it receives no response within the 30-day timeframe.

Every covered entity and business associate is eligible to receive the pre-audit screening email and to be entered into the audit selection pool. However, at this point, we believe the screening e-mail is being sent to entities who have filed a breach notification report with OCR. Based on the responses to the pre-audit questionnaire contained in the screening e-mail, OCR will choose a representative sample of auditees. Entities will be notified if selected.

Phase 2 audits will target areas of frequent non-compliance with HIPAA, such as risk management, privacy practices, individual access to protected health information ("PHI"), breach notifications, and electronic security. Most audits will not involve site visits, though some may. Once an entity is selected for the audit process, it has only 10 days to respond to OCR's audit request, submit all requested documentation through OCR's online portal, and provide a listing of its business associates. While OCR has not stated the exact information that will be requested, we suspect the information requests will include, among other things, HIPAA policies, procedures, and plans, listing of systems that house electronic PHI, risk assessment(s), breach notification documents, Notice of Privacy Practices and other HIPAA forms, and a business associate listing.

Depending on an entity's size, the 10-day window may leave little time to compile and provide the requested information. Thus, while receiving the pre-audit screening e-mail does not guarantee that an entity will be audited, it is recommended that receiving entities take

proactive steps to prepare in the event they are ultimately audited. Recommended steps include the following:

- Assemble a HIPAA response team and hold an initial meeting so that everyone may be prepared in the event of an audit. Potential team members may include your privacy officer, security officer, compliance officer, IT department supervisor, and administrator.
- Locate all HIPAA-related materials so that they can be gathered quickly in the event of an audit.
- Review HIPAA policies and procedures to make sure they are up to date, operating effectively, and do not contain any gaps.
- Review HIPAA forms to make sure they are up to date and are being properly used.
- Compile a listing of business associates, which, for larger entities, could take a significant amount of time. There are several pieces of information OCR has indicated it will request with respect to business associates. A template form for gathering this information is available here. While use of the template is not required, it does ensure inclusion of all the business associate information OCR is seeking.
- In relation, confirm that a business associate agreement is in place for each instance where one is required. We have seen some recent enforcement actions whereby covered entities have been fined for not having a business associate agreement in place when one was required.
- Compile and review the latest risk assessment(s) to make sure they are still valid and cover all the systems that house, transmit, and store electronic PHI. (We have seen recent enforcement actions whereby covered entities have been fined for not having a risk assessment or a series of risk assessments that cover all relevant systems.)
- Compile an inventory of systems and system assets that house, transmit, and store electronic PHI.

OCR has indicated that the Phase 2 audits are not designed to determine an entity's compliance with HIPAA. Nonetheless, OCR has retained the right to initiate a compliance review based on information received during an audit. Thus, we believe it is worthwhile to take the steps mentioned above in order to help reduce the risk of a compliance investigation.

For more information on the Phase 2 HIPAA audits, please contact any of the Burr & Forman attorneys listed on the following page.

Howard Bogard
Partner ~ AL
(205) 458-5416
hbogard@burr.com

Richard Brockman
Counsel ~ AL
(205) 458-5175
rbrockman@burr.com

Kelli Fleming
Partner ~ AL
(205) 458-5429
kfleming@burr.com

Jim Hoover
Partner ~ AL
(205) 458-5111
jhoover@burr.com

Chet Hosch
Partner ~ GA
(404) 685-4279
chosch@burr.com

Matt Kroplin
Partner ~ TN
(615) 724-3248
mkroplin@burr.com

Jack Mooresmith
Counsel ~ AL
(334) 387-2072
jmooresmith@burr.com

Angie Smith
Partner ~ AL
(205) 458-5209
asmith@burr.com

Jerry Taylor
Partner ~ TN
(615) 724-3247
jtaylor@burr.com

Chris Thompson
Associate ~ AL
(205) 458-5325
cthompson@burr.com

Rob Williams
Partner ~ FL
(813) 367-5712
rwilliams@burr.com

Tom Wood
Partner ~ AL
(251) 345-8203
twood@burr.com