From: Raines, Jill (HSC)
To:

(
Subject: OCR Alert on HIPAA Audit Controls
Date: Tuesday, January 17, 2017 5:54:54 PM

Good evening –

OCR issued the following Alert this month regarding the audit controls that are required by HIPAA. Please review your HCC’s audit controls against this Alert to ensure you are meeting the audit control requirements. Recall that each HCC must have a procedure in place for regularly auditing user access to its electronic records systems that contain PHI (see HIPAA Security policy 11 – “HIPAA Security Audits”). You may want to consult with your Tier 1/IT Representative as well.

If you have any questions, please contact Valerie Golden or me. As always, thank you for your assistance with HIPAA compliance. We appreciate all you do!

Understanding the Importance of Audit Controls

January 2017

Covered Entities and Business Associates should make sure that they appropriately review and secure audit trails, and they use the proper tools to collect, monitor, and review audit trails. Protecting audit logs and audit trails prevent intruders from tampering with the audit records and protecting their integrity. Not safeguarding audit logs and audit trails can allow hackers or malevolent insiders to cover their electronic tracks, making it difficult for Covered Entities and Business Associate to not only recover from breaches, but to prevent them before they happen.

According to the National Institute of Standards and Technology (NIST), **audit logs** are records of events based on *applications*, *users*, and *systems*, and **audit trails** involve audit logs of *applications, users*, and *systems*. Audit trails’ main purpose is to maintain a record of system activity by application processes and by user activity within systems and applications.

The HIPAA Security Rule provision on *Audit Controls (45 C.F.R. § 164.312(b)*) requires Covered Entities and Business Associates to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI). The majority of information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity which also includes users and applications activity.

Examples of audit trails include:
Application audit trails – Normally monitor and log user activities in the application. This includes

the application data files opened and closed, and the creating, reading, editing, and deleting of application records associated with ePHI.

System-level audit trails – Usually capture successful or unsuccessful log-on attempts, log-on ID/username, date and time of each log-on/off attempt, devices used to log-on, and the application the user successfully or unsuccessfully accessed.

User audit trails – Normally monitor and log user activity in a ePHI system or application by recording events initiated by the user, such as all commands directly initiated by the user, log-on attempts with identification and authentication, and access to ePHI files and resources.

Audit controls that produce audit reports work in conjunction with *audit logs* and *audit trails*. Audit logs and trails assist Covered Entities and Business Associates with reducing risk associated with: reviewing inappropriate access; tracking unauthorized disclosures of ePHI; detecting performance problems and flaws in applications; detecting potential intrusions and other malicious activity; and providing forensic evidence during investigation of security incidents and breaches. As part of this process, Covered Entities and Business Associates should consider which audit tools may best help them with reducing non-useful information contained in audit records, as well as with extracting useful information.

The HIPAA Security Rule does not identify what information should be collected from an audit log or trail or how often the audit reports should be reviewed. When determining reasonable and appropriate audit controls for information systems containing or using ePHI, Covered Entities and Business Associates must consider their risk analysis results and organizational factors, such as their current technical infrastructure, hardware, and software security capabilities. It is imperative for Covered Entities and Business Associates to review their audit trails regularly, both particularly after security incidents or breaches, and during real-time operations. Regular review of information system activity should promote awareness of any information system activity that could suggest a security incident or breach. Access to audit trails should be strictly restricted, and should be provided only to authorized personnel.

Jill Bush Raines
Assistant General Counsel, Office of Legal Counsel
and University Privacy Official
The University of Oklahoma
1105 N. Stonewall Avenue, Suite 221
Oklahoma City, OK 73117-1221
(405) 271-2033
(405) 271-1076 (fax)
jill-raines@ouhsc.edu

CONFIDENTIALITY NOTICE: This email, which includes any files transmitted with it, contains confidential information from University Legal Counsel, is intended solely for the use of the individual or entity to whom it is addressed, and may contain information protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering this email to the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of this email and any attached files.