**POLICY & PROCEDURES**

***Defining the Overall Approach toward Meeting a Requirement***

### **Information System Activity Review §164.308(a)(1)(ii)(D)**

### **Effective Date:** <Month Day, Year>

### **Policy Number:** <If applicable> **Rev.** 0

**Policy:** We must regularly review records of activity on information systems containing ePHI. Appropriate hardware, software, or procedural auditing mechanisms must be implemented on our information systems that contain or use ePHI. Records of activity created by audit mechanisms implemented on our information systems must be reviewed regularly.

**Procedures:** We conduct random audits of the activity on our information systems. Workforce members will not have access to these audits. Systems containing ePHI are only accessible by logging in with unique user ID information. If suspicious activity is identified based upon these reports, it will be investigated and the results of the investigation documented as a security incident and mitigated to prevent future occurrences.

**Details:** Information system activity reviews may include, but are not limited to:

* Verify no unauthorized users have been added; all terminated users have been deleted and no unauthorized logins have been attempted.
* Verify antivirus program is installed and running a scan every night, as well as performing live scanning whenever files are downloaded or accessed. Scan incoming email for viruses.
* Verify firewall is enabled, review firewall logs and determine if there have been any intrusion attempts or rogue programs added to the allow list.
* If network monitoring software is installed, check its logs, and ensure that no suspicious traffic has taken place on the network.
* Review router logs, if applicable, and check to make sure wireless security is up to date (i.e. WPA2). Change the wireless encryption password periodically.
* Verify information systems are up to date with the latest security patches for the operating system and programs by using Windows Update or checking each program for updates.
* Review ePHI system access logs to identify users who have accessed a system, performed changes to the environment and/or installed / removed software, data, files or other operational content. Where appropriate, automation shall be used to identify unauthorized access or login attempts.
* Review all system error alerts and event messages (e.g. system generated security alerts, system notices, error conditions and other events of a security and non-security nature, etc.).
* Retain documentation (e.g. audit logs, audit reports) of the practices in place as evidence of compliance.

**Location of supporting documentation:** If so, identify the document and location it is stored here.

## REVISION HISTORY

| Revision | Date | Initiator | Nature of Change |
| --- | --- | --- | --- |
| 0 |  |  | Initial draft |
| 1 |  |  |  |