

## STEP 4: DETERMINE IF COMPUTER SYSTEM IS CAPABLE OF PROVIDING ELECTRONIC/AUDIT TRAILS; IMPLEMENT AUDIT CONTROL POLICIES & PROCEDURES

Snapshot Compliance Components			
Safeguard	Standard	Implementation Specification	Required vs. Addressable
Technical	Audit Controls Transmission Security	None Integrity Controls	Required Addressable
Administrative	Security Management Process	Information System Activity Review	Required

See Exhibit 3: Sample Audit Trails Policy & Procedure.

See Exhibit 4: Sample Event Record.

In addition to Step 4, “Perform a Risk Analysis”, Step 5 is one of the more crucial steps for practices to implement. The Security Rule **requires** the practice to implement hardware, software, and/or procedural mechanisms that record and examine activity and information systems that contain or use EPHI. The Practice should refer to Exhibit 2 (Risk Analysis) to determine exactly how intensive the audit control function should be.

Some practices will find that their current practice management and electronic medical records software can produce an electronic audit trail. Under these circumstances, Step 5 is quite easy to implement. However, for those practices that are not so lucky, Step 5 may take some time.

Practices should look at their programs that contain EPHI and determine whether or not it can produce an electronic audit trail. Electronic audit trails are computer programs that allow the computer to track, identify, and record which individuals have accessed the computer system and what activities they have performed while using the computer system. In conjunction with other security tools and procedures, electronic/audit trails can provide the practice with comprehensive information about technical, procedural, and managerial aspects of the practice’s security program. An electronic audit trail will be one way to assess activities regarding EPHI contained in the practice’s computer system.

The practice will first need to determine if its computer system (both hardware and software) can be or is already programmed to accomplish certain tasks, such as track computer user actions, reconstruct abnormal operating situations, detect intruders, and identify general problems related to EPHI. Many of the newer practice software products feature electronic audit capabilities. Note that sometimes this component must be activated first. Do not assume that it is working.

## STEP 4 CONTINUED

If the practice determines that its software containing EPHI cannot produce an electronic audit trail, they should contact their vendor to determine if the product will be compliant by April 21, 2005, or prepare to convert to a product that does offer an electronic audit trail as audit controls are **required** by the Security Rule.

If the software is capable of providing an electronic audit trail, make sure the process is activated. Many systems require the administrator to manually “turn on” the function.

The audit trail also serves as a mechanism for employee and workforce accountability as it tracks who and when employees have accessed computer software programs, what programs they have accessed, and what activities they have performed while logged into the computer system. The audit trail should include information to establish and record who accessed the practice’s computer system, when the computer system was accessed, what software programs were accessed, and any other activities that occurred within the system. This is typically done through an “event record.” The event record should, at a minimum, include the following items:

- Type of event. For example, an unauthorized access to a particular portion of the practice management system for which the employee has not been granted permission to access;
- When the event occurred, including time and day (the practice should determine whether its computer system is capable of date and time stamping such events);
- Which User ID is associated with the event;
- What part of the computer system was used to start the event. For example, did an event occur because an employee accessed the billing component of the practice’s system instead of the clinical component of the system?

## Step 4 continued

### **TO DO:**

- ◆ Determine if your computer system can generate an audit trail. Contact practice management and/electronic medical records vendor(s), if applicable, and ask.
- ◆ If the computer software program(s) can generate an audit trail, determine how to activate this function.
  - Activate the computer software program's audit trail function.
  - Review audit reports weekly.
- ◆ If the computer software program(s) cannot generate an audit trail:
  - Contact the computer software vendor(s) and ask if the product will be compliant by April 21, 2005.
  - If the computer software vendor(s) will be compliant by April 21, 2005, prepare to upgrade and activate the program prior to April 21, 2005.
  - If the computer software vendor(s) will not be compliant, begin looking at other software programs that offer electronic audit capabilities. Prepare to convert to the new program prior to April 21, 2005.
- ◆ Designate an individual in the practice to maintain the audit trail process. Ideally, the individual responsible for assigning and maintaining User IDs and access control processes should be different from the individual maintaining the audit trail functions, but in smaller practices, this is not always possible.
- ◆ Create an event record to establish what event occurred, when it occurred, with whom it is associated, and what part of the system was potentially compromised. (See Exhibit 4).
- ◆ Develop policies and procedures to address conducting and implementing audit trails. (See Exhibit 3).

## STEP 4 CONTINUED

### NOTE:

- ◆ Electronic audit capabilities are **required** by the Security Rule
- ◆ If the computer software program(s) is/are **not** capable of an audit trail, the practice will need to consult with its computer software program vendor(s) and/or an information technology consultant to discuss additional technology solutions.
- ◆ The computer software programs that store EPHI must be able to produce the electronic audit report. It is not required for your computer system in general.
- ◆ Software conversions are time consuming and not always easy. Take into consideration that your workforce will have a learning curve to address. If a conversion is necessary, prepare to schedule this task at least six (6) months prior to April 21, 2005. Do not attempt to activate a new system on April 21, 2005.
- ◆ Comprehensive audit trail policies and procedures should include several important components, including the ability to:
  - identify and track which employees accessed the practice's computer system, when they have accessed it, what they accessed, and what (if any) actions were taken by those individuals (e.g., changes to EPHI);
  - assist in detecting unauthorized access to the practice's computer system or unauthorized access to software programs that an employee does not have access to;
  - identify problems with the computer system, other than intrusions and
  - reconstruct unfortunate events that may have occurred as a result of unauthorized access to the computer system.
- ◆ Depending on the computer software used to perform it, an audit trail can be tracked and monitored in "real time", i.e., the same time, that the employee logs into the computer and accesses the computer system and its software programs.