3.01

Advanced Privacy Compliance Strategies: Who's Looking – Effective Access Audits of Protected Health Information (PHI)

Cecilia R. Plata, RHIA, CHP
Privacy Officer
Valley Medical Center
Renton, Washington

HIPAA Summit Day I - September 8, 2005
Concurrent Sessions III

Access Audits – What are we talking about?

If you are a Privacy Officer, Security Officer, or a HIPAA team member, you will have to do **focused audits** or **incident-related audits** when a complaint or problem is identified.

That is not what this session is about. In this session we will define a regular, on-going access audit process that is part of your organization's HIPAA plan.

Access Audits – What do we mean?

Regular, ongoing review of user access

to your organization's core systems containing restricted PHI,

to assure access is appropriate

based on the "need to know" principle.

Access Audits – Do I really have to do this?

The Privacy and Security guidelines **do not** specifically require that an organization have regular access audits.

However, they hold an organization responsible for misuse of PHI, and require that "security measures ... be reviewed ... as needed to continue **provision of reasonable and appropriate protection**".

Access Audits – Why Do Them?

Random spot checks or complaint-based audits, **generally miss** the majority of inappropriate intrusions by institutional employees and place the institution at **HIGH RISK**.

Access Audits – Compliance SURPRISES

Records of regular access audits to PHI demonstrate that the organization understands the responsibility and is committed to monitor its staff.

Regular access audits often reveal surprising patterns of misuse or abuse. Appropriate remediation leads to compliance and saves the institution lawsuits, fines, and embarrassment.

Audit Process - please make it as painless as possible.

So, you've been convinced that you need to do regular access audits. Perhaps you are already tracking some IS events, such as multiple attempts to log in, password guessing, etc.

Now how much is required, and how to go about setting up this program. Who, What and When are the next questions.

Who's Looking: Journalism 101

WHO	LOOKED?
WHAT	DID (S)HE DO?
	DID (S)HE SEE?
WHEN	DID (S)HE LOOK?
WHERE	DID (S)HE LOOK?
HOW	DID (S)HE GET IN?
WHY	DID (S)HE GET IN?

Who's Looking: Journalism 101

WHO	LOOKED?	AUTOMATED
WHAT	DID (S)HE DO?	
	DID (S)HE SEE?	
WHEN	DID (S)HE LOOK?	
WHERE	DID (S)HE LOOK?	
HOW	DID (S)HE GET IN?	
WHY	DID (S)HE GET IN?	HUMAN

Who's Looking: Journalism 101

WHO	LOOKED?
WHAT	DID (S)HE DO?
	DID (S)HE SEE?
WHEN	DID (S)HE LOOK?
WHERE	DID (S)HE LOOK?
HOW	DID (S)HE GET IN?

AUTOMATED

Is your system collecting ALL this Information?

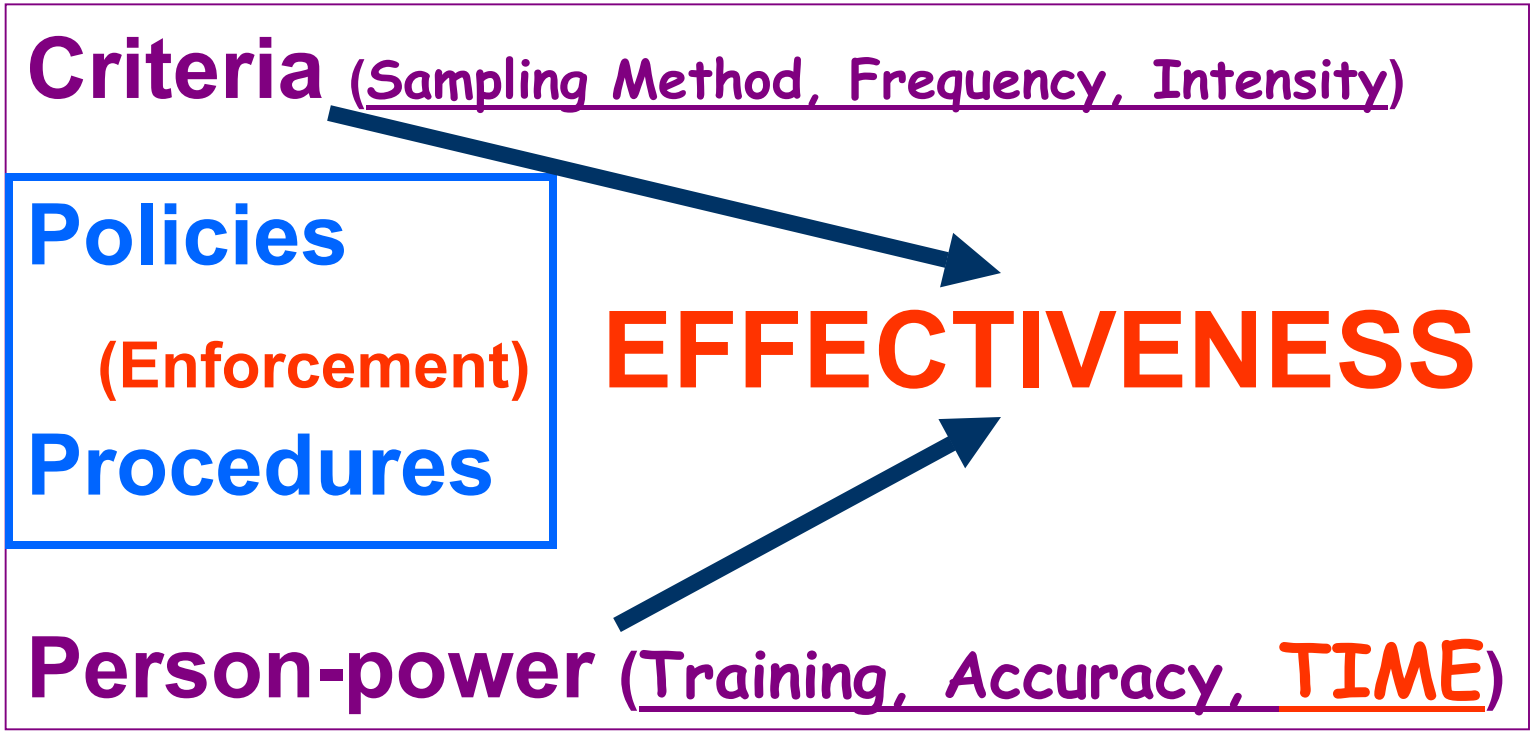
Are the reports organized in a User Friendly Manner?

On-line or Hard Copy?

WHY DID (S)HE GET IN? **HUMAN**

Are your criteria, policies, procedures & person-power in place?

Who's Looking:



Access Audits – Logistics?

We will assume you have already:

- Assigned individual user logins
- Had each user sign a confidentiality agreement (with teeth)
- Had each user's supervisor approve and sign the request for access form.
- Created job-related tables that show access levels based on work responsibility rules.

What systems should we audit?

- Unfortunately in most hospitals, there are multiple systems containing PHI and the number is increasing.
- Start by identifying the core systems that contain the most data and have the greatest use. (*This may depend on where you are in the EHR development*)
- Initially, accept that you cannot audit 100% of the systems that contain PHI.

High Risk Systems First

1. Start with the main Health Information System(s)
2. Prioritize all other independent systems that are accessed directly by some or all staff users
3. Give special attention to Lab., Emergency Dept., Radiology systems, and others that may hold psychiatric or other sensitive information and may be accessed directly or indirectly
4. Lucky are you **IF** you have single-sign on for all these systems!

Do core systems have audit trails?

- Some systems (vendors) do not have audit trail capability and therefore are not HIPAA compliant.
- Some systems may provide limited information qualifying for partial compliance.
- Secondary systems (e.g., Cardiology or Pharmacy) often cannot provide this information.

Breath vs. Depth (Compromise)

The privacy/security team and/or the HIPAA Committee recommend policy concerning the types and volume of audits that should be reasonably performed.

They use the risk analysis profile of the institution and its ability and resources to track, document, and take action.

“Sometimes less is better than more”

Standard Items to Consider

Each Institution has Unique Risks

- Employees as patients
- VIP's
- Physicians as patients (and their families)
- Patients in current headlines & news stories
- Confidential patients (have requested higher level of confidentiality - "no publicity")
- Same name as user (hunt for family members)
- ER browsers (users looking at high volume of ER patients)
- Night browsers (night shift workers)
- High volumes of access by one user (bored employee just grazing)

Deciding What to Audit

Define intrusion categories, then ask if the system(s) can provide such information

EXAMPLE: You want to set up a regular audit of access to employee-as-patient PHI.

Does your database identify when a patient is also an employee?

Automate anything you can

Access audits can be very time consuming unless you automate using validated programmed algorithms for each category.

Easy Automation Targets:

- Same name searches
- Employees as patients
- Patients tagged at registration as VIPs
- Confidential patients

Audit Approaches (like other industries)

Two major approaches of many possible:

- Search for unusual patterns of access
- Random Sampling with full verification of all entries

All operate on an infrastructure of continuous audit trail logs for every entry in every record

Random Audits

- Select certain records (type, number, etc.)
- Investigate and validate **every** access to the record in a standard manner.
- Supervisors verify that each employee had a role-related reason to access that PHI.

Observation: These audits appear routine and are less apt to turn up high risk user behavior. Nevertheless, they give the message that access is monitored for appropriateness.

Search for Patterns - Sample Startup Audit - Who Does What to Whom 1

Let's assume you want to set up a fairly simple audit plan, and will begin by auditing access for employee/patients.

The challenge is identifying appropriate from inappropriate access.

Set up an automated audit that runs nightly and reports all access to employees as patients.

Next morning you have a wonderful report on (appropriate and inappropriate) entries by access points and employee ID.

Now what do you do?

II. Who Does What to Whom?

Some hospitals send these audit results to the employee/patients.

Employees recognize appropriate vs. inappropriate access as their care passed (e.g.,) from the ED, to Lab, case manager, and even when they called Patient Accounts for a question about their bill.

Participation raises staff awareness better than hours of training sessions!

III. Who Does What to Whom?

Routine standard multi-type audits can be screened for selected criteria, and random audit periods can be used for verification.

Example: Choice to investigate only results that appear to show some risk, OR verify every access.

- Cecilia Plata as a user turns up on an audit to have viewed all patients with a last name Plata.
- Audit every user against same last name on database.

Your audit Policy & Procedure need to specify when, who & how will follow-up an incident, and **what will be done about it.**

IV. Who Does What to Whom?

Since the Plata audit finding was not the result of a complaint, the investigation and action plan can be standardized.

- Example: Use email to query Ms. Plata's supervisor to verify, for the HIPAA auditor, a business reason why Ms. Plata accessed multiple patient records with the last name of Plata.
- This appropriately transfers responsibility to the supervisor to do the initial investigation to provide a response.
- It is also important to verify that the supervisor approved the proper access authority for the employee (Ms. Plata).

V. Who Does What to Whom?

- Supervisor determines the employee's "Need to Know." and reports on validity
- The event serves as "Training" for both the employee and the Supervisor
- Everyone knows that "someone is watching"
- "Responsibility through ethics is the goal, responsibility through fear of discovery is a necessary tool"

VI. Who Does What to Whom?

- Supervisor finds and reports no valid reason for entries
- Disciplinary policy and procedure kicks in
- HIPAA program depends on solid P&P for employee sanctions administered with fairness and consistency

Reporting Results

Compliance requires documented audit reports.

Reports go from HIPAA Committee to Compliance Committee.

Results must inform the HIPAA training program and demonstrate continuous improvement.

A sample report shows the total number of accounts reviewed, the number of investigations triggered, and the results of those investigations (see handout example).

Special Challenges

- Physician offices are traditionally a challenge
- Office staff share passwords
- Usual disciplinary actions (suspension/termination) do not apply.
- Physician credentialing is only control avenue
- Medical Staff Bylaws need to include statements of responsibility for confidentiality of PHI.
- When access is granted to physicians they must sign a confidentiality agreement that spells out their responsibilities.

Happy (Audit) Trails to You

- For your use, several sample forms are being distributed today. These are not meant to be perfect forms, but I hope they will be helpful tools you can modify to fit your situation.
- My wish for you is that all access to your systems is appropriate, that 90% of the audit work can be automated, and that your sanction policies get dusty from lack of use!