User Activity Access Monitoring

Frequently Asked Questions

1. ***Who will be audited?***

Everyone who uses Epic, Centricity EMR, Synapse, Meditech, SCM, and any other system that is administered by Yale University or Yale New Haven Health System might be audited.

2. ***Does an audit "hit" mean that I am guilty of violating HIPAA?***

No. An audit hit only shows that someone accessed a record. It raises the question, "was the access required or permitted for work-related purposes? It triggers an investigation, not a disciplinary action. Disciplinary action will be taken only if the investigation reveals that the access was inappropriate.

3. ***Do I have to prove that I am innocent?***

Any audit report that indicates *possible* unauthorized access will be followed up with a thorough investigation. As part of that investigation, you might be asked to explain the circumstances surrounding the access. However, the fact that someone's name appears on an audit report does not mean that they did anything wrong. Nor does it create any presumption of misconduct.

4. ***Do faculty and supervisors know that they are not supposed to use other people's logins?***

All faculty and staff, including faculty and supervisors, promise, every year, to abide by all HIPAA privacy and security policies. This includes the ITS policy on "Appropriate Use," which specifically prohibits password sharing. See ITS Policy No. 1607 , as well as the Yale Standards of Business Conduct and the annual HIPAA assessment

5. ***Will the audits include every Break-the-Glass access?***

No. The goal of the audits is to verify that all access to e-PHI is appropriate. Break-the-Glass ("BTG"; a feature, in Epic, that requires users to explain why they are accessing a record) is triggered based on the kind of record that is accessed. BTG alerts do not indicate whether the access is appropriate. As such, they are of little use, in and of themselves, in discovering unauthorized access; that is, access which is not required or allowed for the performance of your job.

6. ***Does the fact that you printed something show up on an audit?***

Printing is captured in the Epic audit trail. It might not be the basis for an audit "hit," but it might sometimes be helpful in determining why a record was accessed.

7. ***How will I know if I have been audited?***

If the preliminary follow-up investigation does not reveal the reason for what might be unauthorized access, you (and if applicable, your Union representative) will be asked to assist in the investigation. If it is possible to rule out unauthorized access without your involvement, you may never hear of the investigation.

8. ***What if my supervisor doesn't know how I do my job?***

If there is any question about how you do your job, your supervisor will be consulted. The supervisor may call upon others, including Help Desk staff and application "super-users," to gain a more detailed understanding of how you do your job. If that does not work, you, and if applicable, your Union representative will be asked to assist in the investigation.

9. ***How would you investigate an audit "hit" if my "supervisor" is a faculty member?***

Faculty members who supervise staff will be asked to verify that access was required or permitted for the performance of your job. In other words, they will be treated the same as supervisors in any other job classification.

10. ***If I pull up a list of appointments, does every one of the patients' names appear on my activity report?***

They might, depending on the system that you access, and the applications and functions that you use. Please remember, however, that if access to the list of appointments is "required or allowed for the performance of your job," you need not worry that you are out of compliance.

11. ***What qualifications do the audit investigators possess, and how did they earn those credentials?***

Different people, depending on the circumstances, will investigate the audit "hits". The audit investigators will have expertise (acquired through training and experience) in HIPAA privacy and other standards for handling PHI. The investigators will also be required to know (or learn) the basics of how you do your job. There will be times when, upon investigation, they cannot rule out the possibility that access was unauthorized. If that happens, you, and, as applicable, your Union representative would be asked to explain some details of your job, along with the reason for the access.

12. ***If the people who review the audits cannot agree on whether the access is "required or permitted," who will break the tie?***

Disciplinary sanctions for unauthorized access will not be applied if the reviewers cannot agree on whether access was required or permitted. [However, if the access constitutes a violation of some other policy, disciplinary sanctions will be applied accordingly]

13. ***How are you supposed to know whom you're talking with on the phone?***

    You must always verify that callers are who they say they are, and that they are entitled to the information that they are asking for. You can do this by adhering to and documenting the linked best practices. There is no need to follow or document the best practices if you recognize the caller's voice as that of the patient whose information they are seeking. See link to telephone guidance at:http://medicine.yale.edu/ymg/clinical_affairs/practicestandards/index.aspx along with: Guidance on Identity Verification ***What factors will be taken into account in deciding what disciplinary action should be applied?***

The facts and circumstances of the inappropriate access will be taken into account. The effect of any unauthorized access on patient safety or patient care, as well as the reason for

the access, and whether there are previous violations, will be considered, among other factors.

14. How do you define "reasonable alternative" to looking somewhere other than the electronic record? What if the alternative is easy to access, but hard to use?

As always, use your best judgment in determining whether to access information in our patients' records, in electronic, or any other form. The number of available alternatives, the nature and sensitivity of the information, and the potential effect of the access on the patient, should always be considered, along with any other relevant factors.

15. Should I write down the names of all of the people whose records I accessed by mistake?

No, you should not. The better practice would be to continue to do your work, as you normally would, as assigned. It will usually be possible for the investigator to determine the reason for the accidental access based on the way that you usually work, and the records that you accessed around that time.

16. Should I use the "notes" field to document the fact that I accessed a record in error?

No. The systems that will be monitored are designed to capture clinical and billing information only. By keeping the focus on just those two goals, you keep the record concise, making it easier for everyone to find the information that they need.

17. Should I tell my supervisor every time I access a record in error?

No. Your primary obligation is to protect private information. By informing others, you risk broadening the exposure.

18. Can you be fired just for viewing your own record?

No. Unless it interferes with the performance of your job, or in some way compromises patient care or safety, simply viewing your health record, will not lead to disciplinary action.

19. Can I use Epic to look up my appointment times, dates and locations?

While this is not prohibited, the better and likely much more convenient practice would be to access appointment information via the MyChart portal rather than through Epic, directly.

20. Can I use Epic to look up the appointment times for: My small child (under 13)? My teenaged child?

Direct access to children's records, using Epic and other systems, is prohibited. This is true even if you have a legal right to access such information because you are the child's parent or guardian. If your child is age 13 or under, you may access their information via the MyChart portal

21. Can I use Epic to look up the appointment times for: My spouse? An adult family member? My friends, per their request?

No. Direct access to these records, using Epic and other systems, is prohibited. This is true even if you have a legal right to access such information, for example, through a Power of Attorney, conservatorship, or an Authorization to release information. The better practice is to access appointment information via the MyChart portal

22. What do I do if my child, spouse, coworker, next-door neighbor or friend comes to my department when it's my turn to arrive, see, treat or bill patients?

You should follow your department's policies and procedures, which might, or might not prohibit your access to such records.

23. What should I do if a coworker asks me to call up their record so that it does not show up on their audit trail?

Unless accessing a coworker's record is "required or allowed for the performance of your job," you should not do so. If you do access a coworker's record, even at their request, you will subject yourself to possible disciplinary sanctions

24. How do you define "coworker" for the purposes of these audits?

Coworkers include people who work, or have worked, in your department or section, at any level. They also include Yale faculty and staff in other departments, with whom you have regular contact. This could be either through close physical proximity, or because of the nature of your job.

25. Are YNHHS staff considered to be coworkers? Variation: if I access someone's record from YNHH, will it come up on an audit?

Anyone who is listed in both Yale's Oracle human resources database, and YNHHS's human resources database might be the subject of an audit "hit" for either organization.

26. What is the policy on handling faculty or staff records and accounts?

Our policy generally prohibits access to records of faculty and staff or anyone else unless the access is "required or allowed for the performance of your job." If:

- In the normal course of performing your job, you are assigned to work on records or accounts belonging to you coworkers, and if
- You are not subject to any departmental policies that say otherwise,

you will not be subject to disciplinary sanctions simply because you worked with a coworkers' health information.

27. I work in a department that has hundreds of faculty, staff and trainees working in several different sites. Will I be audited for accessing the records of "coworkers" whom I do not know?

For the purposes of these audits, "coworker" is defined in such a way that that should never happen. However, if it does happen, and if you are asked to justify your access, you will have an opportunity to explain not only the reason for the access, but the fact that you do

not know the employee-patient. As always, if you are a Union member, you are entitled to have a Union representative present at that time.

28. If I access a coworker's record by mistake, should I tell my supervisor so that he will know, in the event of an audit?

You are strongly urged not to, for two reasons. One, whenever possible, "hits" that involve employee-patients will be resolved without disclosing PHI to their coworkers or supervisors. So unless preliminary investigation does not make clear the reason for your access, there is no danger of disciplinary sanctions.

The second reason is that, unless the supervisor is asked to help to investigate the "hit," he/she has no reason to know that your coworker received treatment. And if the supervisor has no need to know, your sharing of the information in this circumstance deprives your coworker of *his/her* right to control access to his/her PHI.

29. Will I know if a co-worker has looked at my records?

Yes, but only if someone intentionally or carelessly accesses your health information in a way that compromises the security of your information, and is not required or allowed for the performance of their jobs. On the other hand, if a coworker processes your record or account because it is required or allowed for the performance of their duties, you might never be told.

30. What should I do if I am asked to "Break the Glass"? Does it mean that I did something wrong?

When asked to "Break the Glass", you should take a moment to make sure that you are in the correct record. If you are in the correct record, and if access to that record is "required or allowed for the performance of your job," you should follow the on-screen instructions and proceed as you normally would.