Patient Privacy Intelligence (formerly FairWarning) User Activity Audits FAQ

1. **What is Patient Privacy Intelligence ("PPI")?**

Patient Privacy Intelligence or "PPI" is a monitoring program tool used by Kettering Health ("KH") that interfaces with EPIC and other clinical systems administered by KH. It analyzes user activity to detect potential inappropriate access to patient information.

2. **Why does Kettering Health ("KH") use PPI?**

KH uses PPI because it helps establish a culture of security, privacy, and compliance to expand trust among our patients, providers, and users. PPI helps simplify the lifecycle of information security and privacy by making it easier to detect, investigate, mitigate, and remediate improper user access or behavior.

3. **How does PPI work?**

PPI analyzes EPIC and other clinical systems user activity and flags instances of potential inappropriate access. If potential inappropriate access is flagged, the user's manager is notified. The user's manager and privacy team will review the activity in question and determine whether it was appropriate.

4. **What is an audit?**

An audit is a form of monitoring provided by PPI that shows a user's activity report. The audit will help determine if there was inappropriate access of a patient's health information.

5. **Who is subject to an audit through PPI?**

Everyone who uses EPIC and any other clinical system administered by KH that provides the KH user access to patient PHI is subject to an audit.

6. **Does an audit "hit" mean that I am guilty of violation HIPAA?**

No. An audit hit only shows that someone accessed a patient's 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 to a patient's PHI was not work-related.

7. **Do I have to prove 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 your access of patient information. However, the fact that someone's name appears on an audit does not mean that they did anything wrong. Nor does it create any presumption of misconduct.

8. **Will employees receive PPI training?**

Employees are trained in health information privacy as part of their work-related training and continuing education.

Consequently, employees are aware that they are subject to monitoring when they use systems that contain PHI and will be held accountable for any misconduct.

The PPI audits will be explained in articles in KH publications, online training, and in e-mail messages addressed to all Leadership and Employees.

9. **Is it o.k. to use someone else's login information?**

No. All staff, including leaders, pledge, every year, to abide by all HIPAA privacy and security policies, including:

- IP-KH Access to Information Systems
- IP-KH Disclosures of Protected Health Information to Individuals Involved in Patient's Care
- IP-KH Employee Access to Personal Health Information
- IP-KH Use and Disclosure of PHI for Treatment, Payment, and Healthcare Operations
- IP-KH Using, Requesting, and Disclosing Minimum Necessary Information
- IP-KH Workstation Use and Security

10. **Will you use PPI to audit every Break-the-Glass access?**

No. The goal of the PPI audits is to verify that all access to e-PHI is appropriate. Break-the-Glass ("BTG"); is a feature, in EPIC, that requires users to explain why they are accessing a record, and it is triggered based on the kind of records 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 access that is not required or allowed for the performance of your job.

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

Printing is captured in the EPIC audit trail. It might be the basis for a PPI audit, but it might sometimes be helpful in determining why a record was accessed.

12. **How will I know if I have been audited through PPI?**

If we have questions about whether you access was work-related, we may need to ask you some questions about why you accessed a patient's medical record. At that time, you may be told that we are completing a PPI audit.

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

If there are any questions about how you do your job, your leader will be consulted. Your leader may call upon others, including iSupport staff and application "super-users," to gain a more detailed understanding of how you do your job. If that does not resolve any open questions about your access of patient PHI, your HR Leader Partner will be asked to assist in the investigation, and you may be asked questions about how you perform your job.

14. **How would you investigate an audit if my leader works for Kettering College?**

Faculty members who are also leaders will be asked to verify that access was required or permitted for the performance of an employee's job. They will be treated the same as a leader in any other job classification.

15. **If I pull a list of appointments, does every patient's name 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," that access is appropriate.

16. **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, KH polices and other standards for handling PHI. There will be times when, upon investigation, they cannot rule out the possibility of unauthorized access. If that happens, you, and your Leader would be asked to explain some details of your job, along with the reason for the access.

17. **What factors will be considered in deciding what disciplinary action?**

The facts and circumstances of the inappropriate access will be considered. 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. Other factors may be considered depending on the specifics of the situation.

18. **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.

19. **What if I accidentally access a patient's medical record?**

You should alert your leader and/or Corporate Integrity and continue to do your work. It will usually be possible to confirm accidental access.

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

No. If inappropriate access has been confirmed, it will be documented appropriately but not in Epic.

21. **Can I access my own health record or the health record of a family member or friend with their permission?**

No. While this is not a HIPAA violation, it is in direct violation of KH policy. If you wish to access your own health record for any reason, you should use MyChart. If a friend or family member consents to you accessing their medical record, you should likewise access that information through MyChart. 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 best practice is to access appointment information via MyChart.

22. **What do I do if my family member, friend, or an acquaintance is treated in my department?**

You should follow your department's policies and procedures and only access the patient's PHI for reasons that are directly related to and necessary for the completion of your job responsibilities.

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

Unless accessing a coworker's record in Epic is "required or permitted 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 based on KH policy.

24. **What is KH's policy for access to patient PHI when that patient is a co-worker?**

KH policy prohibits access to patient medical records unless the access is "required or permitted 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 your coworkers, your access will be considered appropriate, unless there is a specific department policy that says otherwise.

25. **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 the 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.